



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

CH-1 of 17 NOV 1997
IN REPLY REFER TO

OPNAVINST 5510.60L
N-09B31
24 May 1991

OPNAV INSTRUCTION 5510.60L

From: Chief of Naval Operations

Subj: SECURITY REGULATIONS FOR OFFICES UNDER THE COGNIZANCE OF
THE CHIEF OF NAVAL OPERATIONS (CNO)

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5540.8L (NOTAL)
(c) OPNAVINST 5530.14B
(d) OPNAVINST 5510.100B (NOTAL)

1. Purpose. To update security policy and procedural guidance for the protection of classified information and materials in the custody of the CNO and his staff or other Department of the Navy Staff for which the CNO has cognizance for security. This instruction is a complete revision and should be read in its entirety. (R)

2. Cancellation. OPNAVINST 5510.60K and OPNAVINST 5510.157

3. Objective. To ensure maximum uniformity and effectiveness in the application of the Information, Industrial, Physical and Personnel Security Program policies by the Office of the Chief of Naval Operations, the Immediate Offices of the Secretary of the Navy and the Department of the Navy Staff Offices.

4. Scope. This instruction is the basic guidance for the Information, Industrial, Physical and Personnel Security Programs for both military and civilian personnel assigned to those Department of the Navy offices for which the CNO has cognizance. By Memorandum of Agreement between the CNO and the Secretary of the Navy, the CNO provides policy and guidance for the protection of classified information and materials in the custody of those personnel assigned to the Immediate Offices of the Secretary of the Navy and Department of the Navy Staff Offices. This instruction supplements reference (a).

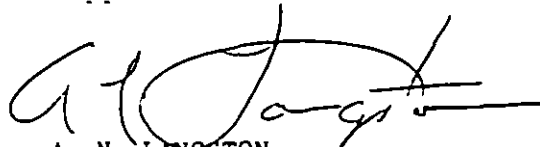
5. Action. All personnel assigned to the offices on distribution for this instruction shall comply with references (a), (b), (c), (d) and this instruction.

17 NOV 1997

6. Reports and Forms

a. The reports identified in paragraphs 0103.2, 0104, 0105, 0205, Exhibit 7A, paragraph 1601, and paragraph 1602 are exempt from reports control by SECNAVINST 5214.2B.

b. Information regarding procurement of the forms prescribed by this instruction is contained in appendix A.



A. N. LANGSTON
Rear Admiral, U.S. Navy
Director, Navy Staff

Distribution:

SNDL	A1	(Immediate Office of the Secretary)
	A2A	(Department of the Navy Staff Offices) (less CNR)
	A6	(Commandant of Marine Corps)
	D1A	(Council of Personnel Boards)
	D1B	(Board for Correction of Naval Records)
	D1C	(Navy Department Board of Decorations and Medals)
	D2A	(Center for Cost Analysis)
	E1A	(Appellate Review Activity)
	E7A	(Audit Service Headquarters)
	E7B	(Audit Service Offices) (NAVAUDSVCAP, only)

All Divisions of OPNAV

Copy to:

SNDL	C25A	(Support Activity Detachments, CNO) (Ft. Richie, only)
------	------	--

24 MAY 1981

TABLE OF CONTENTS

CHAPTER 1
GENERAL REGULATIONS AND ORGANIZATION

<u>PARAGRAPH</u>	<u>PAGE</u>
0101 PURPOSE	1-1
0102 COMMAND RESPONSIBILITY AND AUTHORITY.	1-1
0103 SECURITY ORGANIZATION AND RESPONSIBILITIES.	1-1
0104 REQUESTS FOR INVESTIGATIVE ASSISTANCE	1-10
0105 COUNTERINTELLIGENCE MATTERS TO BE REPORTED.	1-10
0106 EMERGENCY PLAN.	1-12
0107 SECURITY EDUCATION.	1-13
0108 DEBRIEFINGS	1-18
0109 CONTINUING SECURITY AWARENESS	1-20
0110 WAIVERS	1-20
EXHIBIT 1A - SAMPLE DIRECTORATE SECURITY COORDINATOR APPOINTMENT LETTER	1A-1
EXHIBIT 1B - SAMPLE DIRECTORATE TOP SECRET CONTROL OFFICER APPOINTMENT LETTER	1B-1

CHAPTER 2
PERSONNEL SECURITY

0201 BASIC POLICY.	2-1
0202 REQUEST FOR CLEARANCE AND ACCESS.	2-1
0203 EMERGENCY APPOINTMENT TO SENSITIVE POSITIONS FOR CIVILIANS	2-2
0204 CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENTS	2-3
0205 CONTINUOUS EVALUATION OF ELIGIBILITY.	2-3
0206 ADMINISTRATIVE WITHDRAWAL OR ADJUSTMENT OF CLEARANCE	2-4
0207 DENIAL OR REVOCATION OF CLEARANCE/ACCESS FOR CAUSE	2-4
0208 SUSPENSION OF ACCESS.	2-5
0209 CLEARANCE UNDER THE DEPARTMENT OF DEFENSE (DOD) INDUSTRIAL SECURITY PROGRAM	2-6
0210 ACCESS TO CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)	2-6

24 MAR 88

<u>PARAGRAPH</u>		<u>PAGE</u>
0211	DEBRIEFINGS	2-6
	EXHIBIT 2A - SAMPLE REQUEST FOR EMERGENCY APPOINTMENT TO A NONCRITICAL- SENSITIVE POSITION	2A-1
	EXHIBIT 2B - SAMPLE REQUEST FOR EMERGENCY APPOINTMENT TO A CRITICAL-SENSITIVE POSITION	2B-1
	EXHIBIT 2C - PROCEDURES FOR CERTIFYING ACCESS TO CNWDI.	2C-1
	EXHIBIT 2D - BRIEFING/DEBRIEFING CERTIFICATE FOR CNWDI.	2D-1
	EXHIBIT 2E - SAMPLE CERTIFICATION LETTER OF CNWDI "NEED-TO-KNOW"	2E-1
	EXHIBIT 2F - LIST OF AUTHORIZED CNWDI CERTIFYING OFFICIALS.	2F-1

CHAPTER 3 CONTROL AND ISSUE OF BADGES AND PASSES

0301	DEPARTMENT OF DEFENSE BUILDING PASSES	3-1
0302	PROPERTY PASSES	3-4
0303	NAVAL DISTRICT WASHINGTON VEHICLE REGISTRATION PROCEDURES.	3-5

CHAPTER 4 CLASSIFICATION

0401	BASIC POLICY.	4-1
0402	CLASSIFICATION DESIGNATIONS	4-1
0403	FOR OFFICIAL USE ONLY (FOUO).	4-2
0404	ORIGINAL CLASSIFICATION AUTHORITY	4-2
0405	ORIGINAL VS DERIVATIVE CLASSIFICATION	4-4
0406	INDUSTRIAL OPERATIONS	4-4

24 MAY 1981

CHAPTER 5 MARKING

<u>PARAGRAPH</u>		<u>PAGE</u>
0501	BASIC POLICY.	5-1
0502	BASIC MARKING REQUIREMENTS.	5-2

CHAPTER 6 HANDCARRYING OF CLASSIFIED MATERIAL

0601	HANDCARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS.	6-1
0602	PROCEDURES FOR ACQUISITION AND USE OF COURIER AUTHORIZATION CARDS	6-1
0603	AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS	6-2
0604	PROTECTION DURING HANDCARRYING IN A TRAVEL STATUS	6-2
0605	PROCEDURES FOR OBTAINING AUTHORIZATION TO ESCORT OR HANDCARRY CLASSIFIED MATERIAL ON COMMERCIAL PASSENGER AIRCRAFT.	6-3
0606	PROCEDURES FOR CARRYING CLASSIFIED DOCUMENTS ABOARD COMMERCIAL AIRCRAFT.	6-4
	EXHIBIT 6A - CLASSIFIED COURIERS RESPONSIBILITY ACKNOWLEDGMENT	6A-1
	EXHIBIT 6B - SAMPLE COURIER AUTHORIZATION LETTER	6B-1

CHAPTER 7 ACCOUNTING AND CONTROL

0701	BASIC POLICY.	7-1
0702	TOP SECRET.	7-1
0703	SECRET.	7-4
0704	CONFIDENTIAL.	7-5
0705	WORKING PAPERS.	7-5
0706	OTHER REQUIREMENTS.	7-6
	EXHIBIT 7A - PROCEDURES FOR TOP SECRET AUDIT AND INVENTORY.	7A-1
	EXHIBIT 7B - TOP SECRET DISCLOSURE RECORD . . .	7B-1

241-100

CHAPTER 8 **PRINTING, REPRODUCTION AND PHOTOGRAPHY**

<u>PARAGRAPH</u>		<u>PAGE</u>
0801	CONTROLS ON REPRODUCTION.	8-1
0802	TELECOPIERS	8-2

CHAPTER 9 **DISSEMINATION OF CLASSIFIED MATERIAL**

0901	BASIC POLICY.....	9-1
0902	NATO MATERIAL	9-1
0903	TOP SECRET MATERIAL	9-2
0904	SECRET AND CONFIDENTIAL MATERIAL.	9-2
0905	DISSEMINATION TO DOD CONTRACTORS.	9-2
0906	DISCLOSURE TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS	9-2
0907	DISSEMINATION TO CONGRESS	9-2
0908	GENERAL POLICY FOR DISSEMINATION OF INTELLIGENCE	9-2
0909	PROCEDURES FOR THE RELEASE OF INTELLIGENCE TO CONTRACTORS	9-4
0910	SANITIZATION.	9-4
0911	PROHIBITED RELEASE.	9-5
0912	AUTHORIZED SPECIAL MARKINGS WITHIN OPNAV STAFF.	9-6
0913	LIMITED DISSEMINATION CONTROLS (LIMDIS)	9-7
	EXHIBIT 9A - CRITERIA FOR TOP SECRET ORIGINAL CLASSIFICATION AUTHORITIES TO ESTABLISH LIMDIS CONTROLS.	9A-1
	EXHIBIT 9B - SAMPLE LIMITED DISSEMINATION BRIEFING ACKNOWLEDGEMENT	9B-1

CHAPTER 10 **TRANSMISSION OF CLASSIFIED MATERIAL**

1001	BASIC POLICY.	10-1
1002	TOP SECRET.	10-1
1003	SECRET.	10-2
1004	CONFIDENTIAL.	10-4
1005	TELEPHONE TRANSMISSION.	10-5
1006	RECEIPT SYSTEM.	10-6

24 MAR 1991

<u>PARAGRAPH</u>		<u>PAGE</u>
1007	TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS	10-6
1008	TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL.	10-6
1009	TRANSMISSION OF RESTRICTED DATA	10-6
1010	CONSIGNOR-CONSIGNEE RESPONSIBILITY FOR SHIPMENT OF BULKY MATERIAL	10-7
1011	PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION	10-7
1012	ADDRESSING.	10-7
1013	DEFENSE COURIER SERVICE (DCS)	10-8

CHAPTER 11 SAFEGUARDING AND SECURITY STORAGE

1101	RESPONSIBILITY FOR SAFEGUARDING	11-1
1102	SECURITY CONTAINERS	11-1
1103	COMBINATIONS.	11-3
1104	LOCKING PROCEDURES.	11-4
1105	OPNAV LOCKSMITH SERVICES.	11-6
1106	AREAS PROTECTED BY ELECTRONIC ALARM SYSTEMS . .	11-6
1107	OPENING AND SECURING ALARM AREAS.	11-8
1108	UNALARMED WORK SPACES	11-9
1109	CARE OF WORKING SPACES.	11-9
1110	SECURITY CHECK LISTS.	11-11
1111	KEY AND LOCK CONTROL.	11-11
	EXHIBIT 11A - SECURITY CONTAINER INFORMATION (STANDARD FORM 700)	11A-1
	EXHIBIT 11B - ALARMED AREA ACCESS LIST (OPNAV FORM 5512-6).	11B-1
	EXHIBIT 11C - SAMPLE PROCEDURES FOR SECURITY CHECK AT THE END OF THE WORKING DAY . .	11C-1

CHAPTER 12 DESTRUCTION OF CLASSIFIED MATERIAL

1201	GENERAL	12-1
1202	PROCEDURES.	12-1
1203	DESTRUCTION REPORTS	12-1

<u>PARAGRAPH</u>		<u>PAGE</u>
1204	MESSAGE TRAFFIC	12-2
1205	DESTRUCTION OF CMS MATERIAL	12-2
1206	DECLASSIFYING OR CLEARING ADP MEDIA	12-2
1207	EMERGENCY DESTRUCTION PROCEDURES.	12-2
	EXHIBIT 12A - CLASSIFIED MATERIAL DESTRUCTION MANIFEST (OPNAV FORM 5511/57)	12A-1

CHAPTER 13 OPNAV SECURITY WATCH

1301	GENERAL	13-1
1302	DUTIES AND RESPONSIBILITIES	13-1
1303	USE OF ARMS	13-2

CHAPTER 14 VISITS AND MEETINGS

1401	GENERAL	14-1
1402	OUTGOING VISITS	14-1
1403	INCOMING VISITS	14-1
1404	VISITS TO DEPARTMENT OF ENERGY (DOE) ACTIVITIES	14-2
1405	VISITS BY MEMBERS OF CONGRESS	14-3
1406	VISITS BY REPRESENTATIVES OF THE GENERAL ACCOUNTING OFFICE.	14-3
1407	VISITS BY FOREIGN NATIONALS	14-3
1408	CLASSIFIED MEETINGS	14-4
1409	UNCLASSIFIED MEETINGS	14-5
	EXHIBIT 14A - VISITOR CLEARANCE DATA FORM (OPNAV 5521/27).	14A-1
	EXHIBIT 14B - REQUEST FOR VISIT OR ACCESS APPROVAL (DOE F5631.20).	14B-1

CHAPTER 15 INDUSTRIAL SECURITY

1501	GENERAL	15-1
1502	CLASSIFIED CONTRACT	15-1
1503	CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD FORM 254)	15-2

17 NOV 1997

<u>PARAGRAPH</u>		<u>PAGE</u>
1504	CLASSIFIED VISITS TO OPNAV/SECNAVDON STAFF OFFICES BY CONTRACTOR PERSONNEL.....	15-3
1505	DISSEMINATION OF CLASSIFIED MATERIAL TO DOD CONTRACTORS.....	15-4
1506	PROCEDURES FOR ISSUE OF DOD BUILDING PASSES TO DOD CONTRACTOR PERSONNEL.....	15-5
1507	CONSULTANT CLEARANCES.....	15-5
	EXHIBIT 15A - PROCEDURES AND GUIDELINES ON PREPARATION OF DD FORM 254..	15A-1
	EXHIBIT 15B - SAMPLE DD FORM 254.....	15B-1
	EXHIBIT 15C - GUIDELINES FOR ON-SITE CONTRACT PERFORMANCE.....	15C-1

CHAPTER 16

COMPROMISE AND OTHER SECURITY VIOLATIONS

1601	GENERAL.....	16-1
1602	SECURITY VIOLATIONS.....	16-1
1603	ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES AND PUNITIVE ACTIONS.....	16-4
1604	REVIEW OF VIOLATION REPORTS.....	16-5

CHAPTER 17

TERRORISM

1701	INTRODUCTION.....	17-1
1702	RESPONSIBILITIES.....	17-1
1703	THREAT CONDITIONS.....	17-1
1704	BOMB THREAT.....	17-14

CHAPTER 18

LOSS PREVENTION

1801	BASIC POLICY.....	18-1
1802	DD 200 PREPARATION.....	18-2

CHAPTER 19

EMERGENCY PROCEDURES AND NOTIFICATIONS

1901	PURPOSE.....	19-1
1902	PROCEDURES.....	19-1
1903	NOTIFICATIONS.....	19-3

APPENDIX A - PROCUREMENT OF FORMS.....	A-1
--	-----

(A)

[illegible]

14 JAN 83

CHAPTER 1**GENERAL REGULATIONS AND ORGANIZATION****0101. PURPOSE**

This instruction establishes command security policies, responsibilities and procedures to ensure that information classified under the authority of Executive Order 12356 of 2 April 1982 is protected from unauthorized disclosure and that appointment or retention of civilian employees of the command, acceptance or retention of military personnel in the command, granting access to classified information or assignment to other sensitive duties is clearly consistent with the interest of national security and the policies established in references (a) through (d). In the absence of specific reference to requirements here or in other separate directives, the provisions of references (a) through (d) apply.

0102. COMMAND RESPONSIBILITY AND AUTHORITY

1. The Assistant Vice Chief of Naval Operations (OP-09B) is designated to administer the Information, Industrial, Security Education and Training, Physical and Personnel Security Programs for the offices listed on the distribution of this instruction.

2. The Assistant Vice Chief of Naval Operations (OP-09B) will be assisted by the Director, OPNAV Services and Security Division (OP-09B3) in security administration and in enforcement of these programs.

3. The Head, OPNAV Security Branch (OP-09B31) is responsible for the formulation, implementation and enforcement of these security programs, their effectiveness and compliance with all the directives issued by higher authority. OP-09B31 is designated as Security Manager under the provisions of reference (a) and Security Officer under the provisions of reference (c).

0103. SECURITY ORGANIZATION AND RESPONSIBILITIES

1. The OPNAV Security Manager (OP-09B31) is the principal advisor on Information, Industrial, Security Education and Training, Physical and Personnel Security Program policies within the command and is responsible to OP-09B for the management, formulation, implementation and enforcement of security policies and procedures for the protection of classified information

24 MAY 1991

originated by and or under the cognizance of the Chief of Naval Operations, and by Memorandum of Agreement, the Immediate Offices of the Secretary of the Navy and the Department of the Navy Staff Offices. In connection with the duties outlined in references (a), (b) and (c), and to monitor command compliance, disclosure of classified information is authorized and access to all areas shall be given to appropriately identified representatives of the OPNAV Security Branch (OP-09B31) during the conduct of investigations, inspections and security assist visits.

2. Security Inspections and Security Assist Visits

a. Formal Security Inspections shall be conducted for each Assistant Chief of Naval Operations (ACNO), Deputy Chief of Naval Operations (DCNO), Director of Staff Office (DSO), Assistant Secretary of the Navy (ASN) and Department of the Navy (DON) Staff Office once every three years by the OPNAV Security Manager (OP-09B31) to review compliance with the requirements of this instruction and references (a) thru (c). A formal report shall be generated upon completion of inspection and endorsed by OP-09B to the cognizant principal official. Deficiencies will be annotated as requiring action and formal reply to OP-09B of correction of any deficiencies. If required by inspection results, a re-inspection will be conducted.

b. Security Assist Visits will be conducted by the OPNAV Security Manager (OP-09B31) upon request by a designated Security Coordinator. Security Assist Visits will be accomplished in an informal manner and may cover all security requirements or specific items as desired by the requesting Security Coordinator. The purpose of the Security Assist Visit, is to provide on-site assistance in achieving security requirements, not an inspection of compliance with security policy. An informal report of recommendations will be completed at the conclusion of the assist visit and forwarded to the Security Coordinator by the OPNAV Security Manager (OP-09B31).

3. The OPNAV Security Manager is assisted in the performance of assigned duties by the staff listed below:

a. Head, Information Security Section (OP-09B31C) who is responsible for:

(1) The development and monitoring of an Information Security Program to include Classification Management, coordination of the preparation and maintenance of classification guides

24 MAY 1971

issued by the command and ensures compliance with accounting and control requirements for classified material.

(2) The development and monitoring of an Industrial Security Program to encompass the processing of personnel clearances/facility clearances/storage capability for unpaid consultants; is designated "Contracting Officer for Security Matters" for classified contracts with Department of Defense (DOD) contractors, and as such has signature authority on legal contractual documents (DD Form 254s) for such contracts, and authorizes requests for facility clearance/storage capability for contractor facilities.

(3) The development and implementation of the Security Education and Training Program to include conducting security briefings for command personnel, obtaining outside training when and where required and approving and monitoring training provided by Security Coordinators for personnel under their cognizance.

(4) The development and implementation of a command Security Awareness Program. Develops and disseminates newsletters, flyers, posters and other media/materials to enhance the security awareness of all command personnel.

(5) Maintains records of personal/official foreign travel reported by command personnel that identify the travellers route and mode of travel, destination, length of stay, identity of fellow travellers (when applicable) and identity of tour operators (if used).

(6) The development and implementation of a Security Assist Visit Program to provide oversight and assistance on compliance with security requirements to the offices listed on distribution of this instruction. Schedules Assist Visits when requested by Security Coordinators, conducts Assist Visits and provides oral/written reports on findings and recommendations.

(7) Maintains liaison with the command Special Security Officer concerning investigations, access to sensitive compartmented information (SCI) and continuous evaluation of eligibility for personnel/facilities under the DOD Industrial Security Program.

(8) The development and implementation of the NATO/Treaty Material Security Program for those offices, commands and agencies serviced by the CNO NATO Subregistry.

24 MAR 1977

b. Head, Security Operations/Personnel Security Section (OP-09B31D), who is responsible for:

(1) The development, implementation and monitoring of the Personnel Security Program to include the approval and initiation of required investigations for personnel security clearances, the granting of classified access, the review of investigative reports to determine the necessity for further information, the pre-employment check of proposed civilian personnel.

(2) Ensures that all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.

(3) Ensures that access to classified information is limited to those with the need to know.

(4) Ensures that personnel security investigations, clearances and access are recorded.

(5) Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(6) Maintains liaison with the command Special Security Officer concerning investigations, access to sensitive compartmented information (SCI), continuous evaluation of eligibility, and changes to information and personnel security policies and procedures.

(7) Ensures security control of visits to the command when the visitor requires, and is authorized, access to classified information.

(8) Providing 24 hour physical security supervision of DON spaces in the Pentagon.

(9) Routinely conducting inspections of the offices listed on the distribution of this instruction to ensure compliance with DON and command security policies and procedures. Re-inspecting where necessary to ensure deficiencies are corrected.

5-1-67 591

(10) The establishment, control and monitoring of all security areas within the offices listed on distribution of this instruction.

c. Headquarters Automation Division, Assistant for Administration, Under Secretary of the Navy (AAUSN), by Memorandum of Agreement is:

(1) Designated as the ADP Security Officer and the TEMPEST Control Officer.

(2) Is responsible for the ADP Security and TEMPEST Programs.

(3) Ensures that ADP Systems Security Officers are appointed for each ACNO, DCNO, DSO, ASN and DON Staff Office and the major ADP systems.

(4) Provides policy and procedural guidance to ADP System Security Officers and others involved with ADP Security and TEMPEST matters.

(5) Reviews and recommends action on requests for interim authority to operate, accreditation, TEMPEST Vulnerability Assessment Requests, and other ADP Security and TEMPEST documentation.

d. Head, Correspondence Control, Mail and Files Branch (OP-09B34), for OPNAV personnel and the Director, Administrative Services Division, Office of the Secretary, for SECNAV and Department of the Navy Staff Office personnel will assist with the requirement for classification management by reviewing all outgoing classified documents for appropriate classification markings, including page, paragraph/portion and downgrading/declassification statement. Ensure that all outgoing classified material to contractor facilities contains the information and certification required by paragraphs 1012 and 1505 of this instruction.

e. OP-09B31C2 will disseminate all SIOP material to the OP-651E SIOP Control Officer only. Further dissemination of SIOP Material will be determined and accomplished by the SIOP Control Officer only.

4. Each Assistant Chief of Naval Operations (ACNO), Deputy Chief of Naval Operations (DCNO), Director of Staff Office (DSO),

Assistant Secretary of the Navy (ASN) and Director of Department of the Navy (DON) Staff Office, must:

a. Appoint an individual in writing to serve as the Security Coordinator (SC) for their organizational entity (see Exhibit 1A for sample letter). The minimum period of appointment shall be for one year. Assistant Security Coordinators (ASCs) at the division level may be appointed if required to aid the Security Coordinator in performance of his/her duties, however the Security Coordinator is still responsible for those duties.

(1) Security Coordinators will assist in implementing the security programs by:

(a) Ensuring all personnel under their cognizance comply with security regulations.

(b) Serving as a communication link between the OPNAV Security Manager (OP-09B31) and personnel under their cognizance.

(c) Continually monitoring existing security control systems (document, physical, etc.) for effective operation.

(d) Conducting annual refresher security briefings to personnel under their cognizance.

(e) Signing visit requests to outside activities for personnel under their cognizance.

(f) Accounting, control and issuance of courier cards to personnel under their cognizance as outlined in Chapter 6 of this instruction.

(g) Reviewing classified material prepared in their organization for correct classification and marking.

(h) Promoting security consciousness within their organization in support of the command Security Awareness Program.

(i) Ensuring that all assigned personnel have a personnel security clearance/access commensurate with the level of classified information to which they need access.

(j) Establishing visitor control procedures within their offices to preclude unauthorized access to classified information.

(k) Investigating security violations.

(l) Ensuring all assigned personnel attend required security education programs.

(m) Ensuring compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

(n) Briefing newly reporting personnel in local security practices within one week of their assignment and providing the employee with a copy of the local security instruction issued in amplification of this instruction.

(o) Assume the responsibilities of the Assistant Automatic Data Processing Security Officer (ADPSO) in his/her absence.

(p) Annually inspect the offices under their cognizance, using the guidelines contained in Chapter 2, Exhibit 2C of reference (a) and provide a written report of findings to OP-09B31 upon completion of the inspection.

(2) Assistant Security Coordinators are responsible for carrying out the following tasks:

(a) Serving as a communication link between Security Coordinators and cognizant staff personnel.

(b) Reporting security violations to respective Security Coordinators.

(c) Ensuring that personnel under their cognizance conform to the guidance of this instruction and report discrepancies to the Security Coordinator and the immediate supervisor.

(d) Relaying problems or items requiring clarification to Security Coordinators.

(e) Assisting Security Coordinators with other security duties as required (i.e., distribution of Security

27 MAR 1991

Newsletters, security posters, promulgation of policy clarification, security education and training, etc.).

(3) The person appointed as Security Coordinator/ Assistant Security Coordinator may be assigned as a full-time, part-time or collateral duty, but the person designated must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the directorate. The Security Coordinator should be afforded direct access to the Directorate Head. The Security Coordinator/ Assistant Security Coordinator must be a U.S. citizen and have been the subject of a favorably completed Background Investigation (BI). Designation of enlisted personnel or civilians below the GS-11 level is not permitted unless a waiver is granted by the OPNAV Security Manager (OP-09B31). Waiver of the rank/grade requirement is rarely granted. Requests for waiver of the BI requirement, pending completion of the investigation, are usually granted. Directorate Heads are strongly advised to only appoint individuals with previous experience in handling classified material and knowledge of Department of the Navy security procedures.

(4) The usefulness of the Security Coordinator Program is contingent upon effective communication and guidance from OP-09B31. This program does not satisfy all requirements for implementing and maintaining a viable Command Security Program. Instead, because of the size and complexity of the commands supported by the OPNAV Security Manager, it is designed to enhance security awareness, improve operational security practices and serves as a feedback mechanism for the OPNAV Security Manager.

b. Designate in writing (see Exhibit 1B for sample letter), a Directorate Top Secret Control Officer (TSCO) and alternate (ALT-TSCO), (Assistant Top Secret Officers (ATSCOs) may be appointed if required), who will be responsible for the receipt, control, reproduction, destruction, transmission and inventory of all Top Secret material for their directorate. The TSCO will be subordinate to the Security Coordinator (SC). (Assistant Top Secret Control Officers (ATSCOs) at the division level may be appointed if required to aid the Directorate TSCO in performance of his/her duties within the directorate, however the Directorate TSCO is still responsible for those duties and with his/her designated alternate are the only individuals authorized to receipt for Top Secret Material for their directorate. The person designated as the Directorate Top Secret Control Officer/ Assistant Top Secret Control Officer must be an officer, senior

24 Nov 79

noncommissioned officer (E-7, E-8 or E-9) or a civilian employee, GS-7 or above. The Directorate Top Secret Control Officer/ Assistant Top Secret Control Officer must be a U.S. citizen with a final Top Secret clearance who demonstrates mature judgement and is completely familiar with the requirements for protection of Top Secret information and the duties described in paragraph 2-10 of reference (a).

c. Provide a copy of all letters of appointment for SCs, TSCOs and their alternates (including names, applicable code, location and telephone numbers) to OP-09B31 and inform OP-09B31 of changes as soon as they occur. OP-09B31 will maintain an updated database and roster of appointed officials. These individuals shall interface directly with OP-09B31 and are the focal point for their respective directorates on all applicable security matters.

d. Issue Security Procedures for offices under their cognizance in amplification of those contained in reference (a) and this instruction and submit to OP-09B31 prior to implementation for review. Procedures must include, but will not be limited to the following areas:

(1) Establish an accounting and control system for Top Secret and SECRET material to include destruction procedures.

(2) Establish controls on dissemination of classified information to include a review system for distribution lists.

(3) Assign responsibilities for review of classification and associated markings on documents to ensure accuracy and completeness.

(4) Notify all personnel of the location of classification guides and policy on the use of original classification authority.

(5) Internal security training program.

(6) Implement annual in-house inspection program.

(7) Assign an annual clean-out day for the purpose of reducing classified holdings.

24 JAN 1981

0104. REQUESTS FOR INVESTIGATIVE ASSISTANCE

1. The Assistant Vice Chief of Naval Operations (OP-09B) is responsible for all liaison with the Naval Investigative Service (NIS), Office of Personnel Management (OPM), Defense Investigative Service (DIS) and the Defense Protective Service (DPS) in matters of personnel security investigations and civil or criminal investigative matters involving personnel from OPNAV, SECNAV and Department of the Navy Staff Offices except as outlined in paragraph 1602.2g. Utilization of OP-09B as the focal point for such matters is required to avoid delayed processing of cases and possible embarrassment to the Navy, e.g., improper channeling or dissemination of sensitive information.

2. Promptly report all incidents of actual, suspected or alleged criminal offenses to the OPNAV Security Manager (OP-09B31). Investigative assistance, or other action as appropriate, will be promptly initiated to ensure expeditious resolution while at the same time protect the interests of the Navy and the rights of the individual. OP-09B31 will keep appropriate officials advised of pertinent developments as investigation, processing or other required administrative action proceeds.

0105. COUNTERINTELLIGENCE MATTERS TO BE REPORTED

1. Basic Policy. Certain matters affecting national security must be reported to the Naval Investigative Service (NIS) so appropriate counterintelligence action can be taken. All command personnel, whether they have access to classified information or not, will report to the OPNAV Security Manager (OP-09B31) any activities described in this paragraph involving themselves, their dependents or others. OP-09B31 will, in turn, notify NIS.

2. Sabotage, Espionage or Deliberate Compromise

a. Any individual becoming aware of possible acts of sabotage, espionage, deliberate compromise or other subversive activities will report all available information concerning such action immediately to the OPNAV Security Manager (OP-09B31).

b. All command personnel will immediately notify OP-09B31 of any requests, through other than official channels, for classified national defense information from anyone regardless of nationality, or for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, personal data or characterizations of DON

24 JUL 1991

personnel; technical orders, manuals, regulations, command directories or personnel rosters; and information about the designation, strength, mission, combat posture, and development of ships, aircraft and weapons systems.

3. Contacts with Citizens of Designated Countries

a. All personnel will promptly report to OP-09B31C any form of contact, intentional or unintentional, with any citizen, official, office, establishment or entity of a designated country. The term "contact" means any form of encounter, association, or communication, including those made in person, by radio, telephone, letter, or other media of communication, whether for social, official, private, or any other reason. Before contacting or visiting any establishment of a designated country, including those located in the U.S. and friendly countries, personnel will notify OP-09B31C. Subsequent to the contact or visit, individuals must again report to OP-09B31C for debriefing.

b. See Exhibit 5A of reference (a) for a list of designated countries.

c. Contacts with citizens of designated countries are not, in themselves, wrong, against regulations or illegal. However, such contacts must be reported immediately by OP-09B31 to NIS to permit NIS to evaluate the contacts in order to protect the DON from hostile intelligence activities.

d. See also paragraph 0107.6.a, for information regarding a Foreign Travel Briefing.

4. Suicide or Attempted Suicide. When any individual who had access to classified information commits or attempts suicide, the individual's Security Coordinator or supervisor will immediately forward all available information to OP-09B31 for reporting to the NIS and CNO (OP-09N). The report will, as a minimum, set forth the nature and extent of the classified information to which the individual had access and the circumstances surrounding the suicide or attempted suicide.

5. Unauthorized Absentees. When any individual who has access to classified information is in an unauthorized absentee status, the individual's Security Coordinator or supervisor will notify OP-09B31 and conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that his/her absence may be inimical to the interests of national security. The results of this report will be

24 JUN 1977

submitted to OP-09B31. If the inquiry reveals such indications, OP-09B31 will report all available information to the NIS for action.

6. Foreign Travel

a. All command personnel possessing a security clearance are required to report to OP-09B31C all personal foreign travel in advance of the travel being performed. Supervisors will keep this reporting requirement in mind when they are approving leave for their personnel and ensure individuals report to OP-09B31C. Personnel will be reminded of this reporting requirement during orientation security briefings and annual refresher security briefings.

b. See also paragraph 0107.6.a, for information regarding a Foreign Travel Briefing.

c. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel) or the failure to report such travel indicate the need for investigation, OP-09B31 will refer the matter to NIS for action.

0106. EMERGENCY PLAN

1. Emergency procedures for protecting or removing classified material in the event of natural disaster, civil disturbance or enemy action will be followed as outlined in sub-paragraphs 2 and 3 below.

2. The Navy Continuity of Operations Plan (U) (NAVCOOP), (SECNAVINST S3030.4) discusses prepositioning duplicate records essential to continuity of operations during war/emergency situations. Essential records not prepositioned may be hand-carried in accordance with reference (a).

3. In case of evacuation due to fire or natural disaster, individuals in vaults accredited for open storage should evacuate and last person lock combination lock on door only (do not try to set alarm in secure.) For those personnel who have security containers only, put all classified working papers in security containers and lock. The OPNAV Security Force along with the Defense Protective Service (DPS) will provide perimeter protection of areas involved.

24 MAR 60

0107. SECURITY EDUCATION

1. **Basic Policy.** Department of the Navy Policy requires that all commands which handle classified information establish and maintain an active Security Education Program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures.

2. **Purpose Of The Program**

a. The Security Education Program instills an appreciation of the need for protecting classified information from hostile threats, what those threats are and ways used by the threats to obtain classified information. The Information and Personnel Security Programs provide a framework for protection of information the controlled dissemination of which is essential to national security. In an open society, such as that of the United States, disclosure outside authorized channels is tantamount to disclosure to a hostile intelligence service.

b. The purpose of the Security Education Program is to make sure that all personnel understand the need to protect classified information and know how it is to be safeguarded. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified information becomes a natural element of every task.

3. **Responsibility**

a. The Head, Information Security Section (OP-09B31C) is responsible for administering the Security Education Program via Security Coordinators and their assistants. OP-09B31C will assist Security Coordinators in obtaining training materials and training aids; the Security Coordinators will conduct the training. Duties and security topics are discussed below.

b. Supervisors are responsible for two security education functions:

(1) Identifying security requirements applicable to their organizational elements.

(2) Ensuring that personnel under their supervision understand and comply with the security requirements for their particular assignments.

24 MAY 1991

4. **Scope.** Some security education will be provided to all command personnel, whether or not they have access to classified information. More extensive education will be provided for those who do have access.

5. **Minimum Requirements**

a. **Indoctrination**

(1) Everyone who enters the Navy and the Marine Corps needs to have a basic understanding of what classified information is, and why and how it is protected.

(2) Normally this basic indoctrination is done during training at the time of accession. However, since past experience has proven that new personnel are not usually provided any indoctrination training prior to reporting aboard the command and no record is available for this command to verify or maintain regarding any prior security indoctrination, all new personnel will receive this security indoctrination as a part of their check-in process with their respective Security Coordinator. This will afford the Security Coordinator an opportunity to emphasize specific security information required by the individual pertaining to his/her duties and physical office location, familiarizes the individual with his/her Security Coordinator for future use and eliminates the employee from having to report for numerous check-in type meetings.

(3) A written Security Indoctrination Briefing stating basic security requirements will be given to each employee by the OPNAV Security Branch (OP-09B31) on the day of check-in. In addition, within one week, the Security Coordinator must brief the employee on basic principles of security and local security procedures within their respective directorate/division and must certify that the briefing has been accomplished by countersigning the Security Indoctrination Certification and Request for Clearance memo.

(4) As a minimum the indoctrination training will include sufficient information to make the individual aware that:

(a) Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;

24 MAY 1991

(b) Classified material will be marked to show the level of classification (Top Secret, Secret or Confidential);

(c) Classifiable information is information which should have been marked as classified, but which, as a result of negligence, time constraints, error, lack of opportunity or oversight, has not been marked as classified;

(d) Only those who have been officially and specifically authorized may have any access to classified information;

(e) Classified material must be stored and used in security areas, protected during transfer from one area (or command) to another, and destroyed by authorized means;

(f) Any breach of security must be reported to their Security Coordinator or the OPNAV Security Manager;

(g) Any contact in any form with any citizen of a designated country must be reported (see paragraph 0105.3); and

(h) Any attempt by an unauthorized person to solicit classified information must be reported to their Security Coordinator or the OPNAV Security Manager.

b. Orientation

(1) Each person who will have access to classified information will be given an orientation briefing as soon as possible after reporting aboard or being assigned to duties involving classified access.

(2) OP-09B31C will present regularly scheduled command orientation briefings. Personnel will be scheduled for orientation briefings as part of their check-in with OPNAV Security.

c. On-The-Job Training

(1) Supervisors are responsible for training subordinates on knowing the security requirements impacting on the performance of their duties. On-the-job training is the phase of security education when application of specific security procedures is learned.

24 MAR 1977

(2) Supervision of the on-the-job training process is critical. Leaving subordinates to learn by trial-and-error is costly to security, as is assuming they know how classified information is to be protected. In reviewing compromise/violation reports, it is often found that fault lay with the supervisor who assumed that subordinates knew what they were supposed to do. Examples include assigning duties as "accounting and control clerk", particularly as a substitute without instruction on proper accounting and receipt procedures, assigning responsibilities for mailing classified material without training in the preparation and transmission of classified material, designating Top Secret control duties without reviewing control requirements, responsibility for originating classified information without training in proper classification procedures, classification guides or their location within the office and for assigning duties for typing classified material without any instruction on what classification markings are and placement on typed documents.

d. Annual Refresher Briefing

(1) At least once a year command personnel will receive a refresher briefing covering these topics or related issues:

- (a) Recent counterintelligence highlights
- (b) Examples of common security violations
- (c) Procedural changes
- (d) Terrorism
- (e) Reporting requirements

(2) The refresher briefing does not have to cover the whole subject of security. Since it is unlikely that it will be possible to schedule everyone in the directorate at the same time, the refresher briefing will be more effective if it is tailored for a particular group. For example, the briefing should include guidance on policy and procedural changes, plus required counterintelligence reminders. For clerical personnel concentrate on the preparation of classified material, or for those who draft classified documents, review the procedures for classifying and marking material. A review of the requirements governing handcarrying classified material would be appropriate for those who are most likely to travel on command business. A

24 MAY 1981

review of clearance criteria and adjudicative policy would be appropriate for supervisors of cleared personnel.

(3) Security Coordinators will handle scheduling requirements, provide the briefings and notify OP-09B31C in writing of the full names, SSN and briefing date for attendees.

e. Counterespionage Briefing. Attendance is required every two years for those who have access to information classified at the Secret level or above. The briefing is conducted by a Naval Investigative Service (NIS) Agent and is designed to enhance awareness of personnel to the hostile intelligence threat. OP-09B31C will routinely coordinate with NIS and arrange these briefings.

6. Special Briefings. The following special briefings must be scheduled/attended as follows:

a. Foreign Travel Briefing

(1) Any individual who has had access to classified information who plans to travel to or through a designated country or to attend a meeting, in the United States or elsewhere, in which representatives of designated countries are expected to participate shall report these plans to his/her Security Coordinator, who must schedule a defensive briefing with OP-09B31C. Individuals intending cruises on Soviet ships, which have become available recently, also require this precautionary briefing. Exhibit 5A of reference (a) is a listing of designated countries.

(2) Personnel will be made aware of the fact that this is a required briefing by their Security Coordinator and during other required security training and that they are responsible for advising OP-09B31C through their Security Coordinator when a situation requiring a foreign travel briefing arises. However, failure of the OPNAV Security Manager or the individual's Security Coordinator to inform any individual of that individual's responsibilities under this section does not excuse that individual from his/her responsibility to be familiar with and comply with reference (a) or this instruction, specifically this reporting requirement.

(3) When the individual returns, he/she must be debriefed by OP-09B31C to provide the opportunity to report any incident - no matter how insignificant it might have seemed -

14 JUL 1991

that could have security implications. OP-09B31C will maintain record of the brief and debrief for follow-up.

(4) Those who frequently travel (more than once a month) or attend meetings or host meetings for foreign visitors need not be briefed at each occasion. However, such individuals will be provided a thorough briefing at least once every six months, and a general reminder of security responsibilities before each such activity. This does not excuse the individual however, from reporting the travel itself.

(5) The foreign travel briefing is only required for those who have had access to classified information but it may be given to dependents, or others without access, upon request of command sponsor. Briefings to dependents, or others without access, will be unclassified.

b. North Atlantic Treaty Organization (NATO) Briefings. All personnel who require access to NATO information must be briefed in accordance with reference (d) on NATO security procedures before access may be granted. This briefing is given by OP-09B31C2 or the NATO Control Points approved and briefed by OP-09B31C2.

c. Single-Integrated Operational Plan Extremely Sensitive Information (SIOP-ESI). A special briefing is required before access to SIOP-ESI may be granted. A briefing (and debriefing) certificate, as required by paragraph 3-11.1c of reference (a) must be executed. This briefing (and debriefing) is given by OP-651E (SIOP Control Officer).

d. Sensitive Compartmented Information (SCI). The Special Security Officer (OP-092Z/SSO) is responsible for briefing those who are to have access to SCI.

e. Critical Nuclear Weapons Design Information (CNWDI). Refer to paragraph 0206 of Chapter 2 for information concerning the briefing/debriefing requirements for access to CNWDI.

0108. DEBRIEFINGS

1. Those personnel who have had access to classified information must be debriefed by their Security Coordinator under the following conditions:

a. Prior to termination of active military service or civilian employment, or temporary separation for a period of

24 MAY 1981

sixty (60) days or more, including sabbaticals and leave without pay.

b. At the conclusion of the access period, when a Limited Access Authorization has been granted.

c. When security clearance is revoked for cause.

d. When security clearance is administratively withdrawn.

2. A debriefing will also be given, and a Security Termination Statement executed, when a member of the command inadvertently has substantive access to information which he or she isn't eligible to receive.

3. At the debriefing, it should be made clear to the individual that all classified material in his or her possession must be returned; that he or she may never divulge classified information, orally or in writing, to any unauthorized person or in judicial, quasi-judicial, or administrative proceedings and that there are severe penalties for disclosure; and that he/she must report to the NIS, (or to the Federal Bureau of Investigation (FBI) or nearest DOD component if no longer affiliated with the DON), without delay, any attempt by an unauthorized person to solicit classified information. If it can be narrowed down, remind the individual of the kinds of information to which he/she had access which are classified. A sample debriefing is Exhibit 3C of reference (a).

4. The individual will then be required to read the provisions of the Espionage Act and other criminal statutes in Appendix F of reference (a), read the Security Termination Statement and sign it. (A sample Security Termination Statement (OPNAV Form 5511/14) is Exhibit 3D of reference (a)). The witness to the signature then signs the Security Termination Statement. If someone refuses to execute the Security Termination Statement, ensure the individual is debriefed and stress the fact that refusal to sign doesn't change the obligation to protect classified information from unauthorized disclosure. Annotate the statement to show that the individual refused to sign and send a copy to OP-09B31.

5. The Office of the Secretary of Defense has specifically directed that Security Termination Statements shall be executed by senior officials (flag and general officers, GS-16s and above,

24 JAN 1991

Senior Executive Service and equivalent positions.) The immediate senior of the senior official will ensure that the statement is executed and that failure to execute the statement is reported immediately to the Deputy Under Secretary of Defense for Policy via Chief of Naval Operations (OP-09N).

6. Place the original Security Termination Statement in the individual's official personnel record for permanent retention.

0109. CONTINUING SECURITY AWARENESS

The OPNAV Security Manager (OP-09B31) will periodically disseminate security posters, flyers, bulletins and newsletters to enhance security awareness of command personnel. Security Coordinators and supervisors should ensure these items are displayed/routed to cognizant staff personnel for the widest dissemination throughout the command. Suggested security news items are welcome. The command goal is to strengthen security through knowledge and understanding.

0110. WAIVERS

1. When an ACNO, DCNO, DSO, ASN or Director of DON Staff Office finds that fulfilling the requirements of this instruction results in an untenable sacrifice of operating efficiency, or when there are other good and sufficient reasons, a waiver of a specific requirement may be requested from OP-09B31. Requests for waiver of DON policy requirements will be reviewed by OP-09B31 and forwarded to CNO (OP-09N) for approval/disapproval if appropriate and properly justified. As guidance, the following information concerning waivers is provided:

a. The command currently has been granted a waiver of the requirement to maintain accountability and control records and record the destruction of routine short-life message traffic received from the Joint Communications Center. If the message traffic is received by other means, retained for file, reproduced or further disseminated, then the accountability and control requirements and destruction procedures outlined in Chapters 7 and 12 apply.

b. Requests to waive all accounting and control requirements for Secret material are never granted by OP-09N.

2. Each request for waiver must give the reason why the requirement cannot be met and describe the alternative procedures.

14 MAY 1961

EXHIBIT 1A

S - A - M - P - L - E

5510

Date

From: Directorate Head
To: Individual Appointed (full name, office code, location and telephone number)

Subj: DESIGNATION AS DIRECTORATE SECURITY COORDINATOR

Ref: (a) OPNAVINST 5510.60L
(b) OPNAVINST 5510.1H

1. In accordance with reference (a), you are appointed as Directorate Security Coordinator. Your period of appointment will be for at least one year, from _____ until _____. You will be notified of any change in this appointment.

2. You will be required to become thoroughly familiar with many aspects of references (a) and (b) as applied to your specific organization. Along with the OPNAV Security Manager and the OPNAV Security Officer (OP-09B31), you are to make certain that security policies are effectively implemented in a cohesive manner. You will ensure that all personnel in the directorate, especially those assigned special security responsibilities, are advised of any security policy changes.

3. For effective management of the program, you shall:

a. Serve as the Directorate Head's advisor and direct representative in matters pertaining to security, and serve as the communication link between OPNAV Security (OP-09B31) and Directorate personnel.

b. Develop written Directorate Security procedures, including an emergency plan. These procedures should be consistent with reference (a) and cover those items listed in paragraph 0103.4 of reference (a).

c. Coordinate and implement the security education program in the Directorate.

24 MAR 1987

d. Ensure that threats to security, compromise and other security violations are promptly reported, recorded and, when necessary vigorously investigated. Monitor existing security control systems (document, physical, etc.) for effective operation.

e. Administer the Directorate's program for classification, declassification and downgrading of classified information.

f. Ensure Directorate compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

g. Formulate and coordinate Directorate Physical Security measures for protection of classified materials.

h. Ensure security control of classified visits to and from the Directorate. You are also required to have, by direction, signature authority for outgoing visit requests from the Directorate.

i. Ensure protection of classified information during unclassified visits to the Directorate.

j. Ensure, where applicable, Directorate compliance with the Industrial Security Program for classified contracts with DoD contractors.

k. Ensure that all Directorate personnel who are to handle classified information or to be assigned to other sensitive duties, are appropriately cleared, and that requests for security clearances are properly prepared, submitted and monitored.

l. Ensure that access to Directorate classified information is limited to those with a need-to-know.

m. Coordinate the Directorate's program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

n. Ensure that appropriate security briefings/debriefings are scheduled and given by OP-09B31C to every individual in the Directorate departing on or returning from foreign travel involving countries listed in Exhibit 5A of reference (a). Also ensure that required briefings are provided to personnel before attending meetings anywhere it can be anticipated that representatives

24 MAY 1991

from those countries listed in Exhibit 5A of reference (a) will participate.

o. Ensure that every required precaution is taken to prevent unauthorized disclosure when Directorate individuals are hand-carrying classified material within the Command in the performance of daily duties, or outside the Command in a travel status.

p. Ensure that adequate security measures are provided for in advance, during, and after any Directorate meetings or conferences where classified information will be disclosed.

q. Evaluate the effectiveness of the Security Program in the Directorate by conducting annual division security inspections per guidelines contained in Exhibit 2C of reference (b) as they pertain to Directorate security.

r. Assist OP-09B31 in the identification of potential problems affecting the Security Program and report such items to OP-09B31.

s. Assist the OPNAV Security Manager (OP-09B31) with other security duties as required.

t. Perform those duties assigned to Assistant Security Coordinators in their absence.

4. I request your support and professionalism in helping to carry out this vital program. At the forefront of the thoughts of all Directorate personnel should be that each person, military or civilian, in this Command is individually responsible for our national security through compliance with security regulations.

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (OP-09B31)

24 MAY 1991

EXHIBIT 1B

S - A - M - P - L - E

5510
Date

From: Directorate Head
To: Individual Appointed (full name, office code, location and telephone number)

Subj: DESIGNATION AS DIRECTORATE TOP SECRET CONTROL OFFICER

Ref: (a) OPNAVINST 5510.60L
(b) OPNAVINST 5510.1H

1. In accordance with reference (a), you are appointed as Directorate Top Secret Control Officer. Your period of appointment will be for at least one year, from _____ until _____. You will be notified of any change in this appointment.

2. You will be required to become thoroughly familiar with many aspects of references (a) and (b) as applied to your specific organization. Along with the Directorate Security Coordinator and the OPNAV Security Manager (OP-09B31), you are to make certain that security policies applicable to Top Secret material are effectively implemented in a cohesive manner. You will ensure that all personnel in the directorate with Top Secret access, especially those assigned Top Secret control responsibilities, are advised of any security policy changes.

3. For effective management of the program, you shall:

a. Serve as the Directorate Head's advisor and direct representative in matters pertaining to Top Secret control, and serve as the communication link between the OPNAV Security Manager (OP-09B31) and Directorate personnel.

b. Develop written Directorate Top Secret Control procedures to be included in the Directorate Security procedures. These procedures should be consistent with references (a) and (b).

c. Administer the Directorate's program for classification, declassification and downgrading of Top Secret information.

24 MAY 1991

d. Ensure Directorate compliance with accounting and control requirements for Top Secret material, including receipt, distribution, inventory, reproduction and disposition.

e. Ensure that all Directorate personnel who are to handle Top Secret information are appropriately cleared.

f. Conduct the annual inventory required by reference (a).

g. Ensure that access to Top Secret information is limited to those with a need-to-know and records of disclosure are properly executed.

h. Evaluate the effectiveness of the Top Secret Control Program in the Directorate by conducting annual division security inspections per the guidelines contained in Exhibit 2C of reference (b) as they pertain to Top Secret control.

i. Perform those duties assigned to Assistant Top Secret Control Officers in their absence.

4. I request your support and professionalism in helping to carry out this vital program. At the forefront of the thoughts of all Directorate personnel should be that each person, military or civilian, in this Command is individually responsible for our national security through compliance with security regulations.

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (OP-09B31)

24 MAY 1991

CHAPTER 2**PERSONNEL SECURITY****0201. BASIC POLICY**

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of his/her loyalty, reliability and trustworthiness and the individual has executed a "Classified Information Nondisclosure Agreement" (Standard Form 312). The initial determination will be based on a personnel security investigation (PSI) appropriate to the access required or to other considerations of the sensitivity of the duties assigned.

2. Only the OPNAV Security Manager (OP-09B31) is authorized to request PSIs on personnel assigned to offices under the cognizance of the CNO for security programs. The only exception to this policy is that the OP-092Z/SSO office has complete responsibility for PSIs on individuals who require SCI access.

3. Personnel Security investigative requirements are contained in Chapter 21 of reference (a). Only the minimum investigation to satisfy a requirement may be requested.

0202. REQUEST FOR CLEARANCE AND ACCESS

1. All civilian and military personnel reporting aboard OPNAV, SECNAV and the DON Staff Offices are required to check-in with the OPNAV Personnel Security Unit (Room 4A662). During the check-in process, each individual is issued a security indoctrination package to be completed by the individual and turned over to their Security Coordinator for further action.

2. Security Coordinators shall review this package and request the required degree of clearance/access from OP-09B31 for the new member on the proper memorandum provided with the package.

3. The Head, Security Operations/Personnel Security Section (OP-09B31D) will initiate required action to request the proper clearance from the Central Adjudication Facility (CAF), and provide the cognizant Security Coordinator with a copy of the Personnel Security Action Request (OPNAV 5510/413) provided the individual has the correct up-to-date investigation required for

24 MAY 1991

clearance requested. If the individual does not have the correct up-to-date investigation, OP-09B31D will contact the individual for initiation of required paperwork for either a new investigation or a periodic re-investigation (PR) as applicable.

WARNING: Until the Security Coordinator has received notification from OP-09B31D that an individual's clearance/access has been granted, **ACCESS TO CLASSIFIED INFORMATION IS NOT AUTHORIZED.** Access without this notification constitutes a security violation.

4. When a final clearance has been granted by the CAF, a message is sent to OP-09B31D and upon receipt OP-09B31D will take the following action:

a. A copy of the message is sent to the cognizant Security Coordinator for records purposes.

b. A copy of the message is filed in the individual's official personnel record.

0203. EMERGENCY APPOINTMENT TO SENSITIVE POSITIONS FOR CIVILIANS

1. When an appointee does not have an investigative basis for appointment to a non-critical sensitive position, an emergency appointment to a non-critical sensitive position may be granted and interim clearance may be requested. ACNOs, DCNOs, DSOs, ASNs and Directors of DON Staff Offices must submit an emergency appointment letter including a request for interim clearance (See example in Exhibit 2A) to the OPNAV Security Manager, (OP-09B31) with information copies to Secretariat Headquarters Civilian Personnel Office (S/HCPO) and the cognizant Security Coordinator.

2. A pre-appointment Background Investigation is required for a critical sensitive position. In an emergency, a critical sensitive position may be occupied pending completion of a Background Investigation by Defense Investigative Service (DIS) only if a valid ENTNAC, NAC, or NACI has been favorably completed. An emergency appointment letter including a request for interim clearance (See example in Exhibit 2B) must be submitted to the OPNAV Security Manager (OP-09B31) with information copies to S/HCPO and the cognizant Security Coordinator. There is no provision for appointment to a critical sensitive position when the individual does not have any valid investigative basis.

24 JAN 1981

0204. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENTS

1. A Classified Information Nondisclosure Agreement (Standard Form (SF) 312) is to be executed by all cleared government and non-government personnel as a condition of access to collateral (non-compartmented) classified information.

2. All personnel (military or civilian) are required to execute a SF 312 as a part of their check-in procedure with the OPNAV Security Branch (OP-09B31D), unless verification can be made that a valid Classified Information Nondisclosure Agreement has previously been executed and remains valid for the individual.

3. Refusal to execute the SF 312 will be grounds for denial of access to classified information.

0205. CONTINUOUS EVALUATION OF ELIGIBILITY

1. Personnel security responsibilities don't stop once a favorable personnel security determination is made. Any person having knowledge or information reflecting on an individual's loyalty, reliability and trustworthiness from a security perspective, will immediately report the full particulars and circumstances to the OPNAV Security Manager (OP-09B31) for evaluation and/or further investigation.

2. S/HCPD, Security Coordinators and assistants, command legal staff officials and in particular supervisors are cautioned that information which could place an individual's loyalty, reliability and trustworthiness in question has to be evaluated from a security perspective and are hereby required to familiarize themselves with the adjudication policy contained in Exhibit 22A of reference (a). Behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct is potentially significant to an individual's security status and information concerning these issues must be immediately reported to OP-09B31.

3. Co-workers have an equal obligation to advise their supervisor, Security Coordinator or OP-09B31 when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

1 MAY 1981

0206. ADMINISTRATIVE WITHDRAWAL OR ADJUSTMENT OF CLEARANCE

1. The security clearance of an individual will be administratively withdrawn, without prejudice, when there is no need for access to classified information in connection with his/her official duties. Clearance will be administratively adjusted when the level of access required for official duties changes, provided the appropriate investigative basis for the required clearance exists.

2. When a clearance is administratively withdrawn, the individual will be debriefed by the cognizant Security Coordinator in accordance with paragraph 3-11 of reference (a). The executed Security Termination Statement will be filed in the official personnel record.

3. Administrative withdrawal or lowering of a security clearance is not authorized for cause (i.e., when disqualifying information about the individual is known). A resulting unfavorable personnel security determination will result in denial or revocation of clearance.

4. When a security clearance is administratively withdrawn or lowered, the Head, Security Operations/Personnel Security Section (OP-09B31D) will submit an OPNAV Form 5510/413 to the CAF to show that the action was taken administratively and without prejudice to the individual.

5. A security clearance which was administratively withdrawn or lowered may be reinstated to the previous level of eligibility if access requirements for official duties change. After favorable review of locally available records, clearance level may be adjusted.

0207. DENIAL OR REVOCATION OF CLEARANCE/ACCESS FOR CAUSE

1. When a personnel security determination has been made that an individual does not meet or no longer meets the criteria for a security clearance, the clearance will be denied or revoked for cause by the Central Adjudication Facility (CAF).

2. Denial or revocation of security clearance for cause is an unfavorable personnel security determination, as described in paragraph 22-6 of reference (a). On revocations, the individual will be debriefed in accordance with paragraph 0108 and the Security Termination Statement will be filed in the official personnel record.

24 MAR 88

3. When a DON civilian is incarcerated as the result of conviction for a criminal offense or is absent without leave for a period exceeding 30 days or when a military member is adjudged punitive discharge, is incarcerated as the result of conviction for a criminal offense, or is declared a deserter, the OPNAV Security Manager (OP-09B31) will revoke security access eligibility immediately and without regard to unfavorable action procedures. The report of revocation will be forwarded by the Head, Security Operations/Personnel Security Section (OP-09B31D) to the DON Central Adjudication Facility (DONCAF).

4. A request for security clearance and/or assignment to a sensitive position, following a final unfavorable personnel security determination, may be requested after a reasonable passage of time of the original decision when it is determined that the individual appears able to meet the criteria for clearance/assignment and a need for clearance/assignment exists. A request for eligibility determination must be made to the DON CAF.

5. When a request is received to consider eligibility, following an unfavorable personnel security determination of an individual, the Head, Personnel Security Section will not grant an interim security clearance nor will the requesting office assign the individual to sensitive duties until a final decision is made by the DONCAF.

0208. SUSPENSION OF ACCESS

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the OPNAV Security Manager may decide to limit or suspend access. Limitation or suspension of access for cause may only be used as a temporary measure until the individual's eligibility for access has been resolved.

2. When effecting limitation or suspension of access, the OPNAV Security Manager will:

a. Advise the individual, in person, when limiting or suspending his/her access. The reason for limitation or suspension may or may not be given to the individual, as deemed appropriate by the OPNAV Security Manager;

b. Take steps to ensure that the individual's name is removed from all local access rosters, or limitation noted, and that all coworkers are notified of the limitation or suspension;

24 MAY 1991

- c. Ensure that the combination to classified storage containers, to which the individual had access, are changed; and
- d. Post a notice of limitation or suspension of access in the individual's personnel file, pending final resolution of the individual's eligibility status.

0209. CLEARANCE UNDER THE DEPARTMENT OF DEFENSE (DOD) INDUSTRIAL SECURITY PROGRAM

Information regarding clearance under the DOD Industrial Security Program is contained in Chapter 15.

0210. ACCESS TO CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)

1. Because of the extreme sensitivity of CNWDI, access to and dissemination of CNWDI information must be limited to the minimum number of persons who require it in the performance of their official duties. To meet this objective, and to ensure that policy guidance contained in DOD Directive 5210.2 of 12 January 1975 (NOTAL) and reference (a) is strictly observed, special administrative controls have been established in Exhibits 2C thru 2F to positively identify those personnel requiring access to CNWDI within the offices listed on distribution of this instruction.

2. Certifying officials outlined in Exhibit 2F shall implement the procedures outlined in Exhibits 2C thru 2E for those personnel under their jurisdiction requiring access to CNWDI.

3. Personnel responsible for maintaining personnel clearance and security briefing forms shall notify OP-09B31 of deletions to the listing of authorized personnel (Exhibit 2E) as they occur. The CNWDI Debriefing Certificate, as shown in Exhibit 2D must be completed.

0211. DEBRIEFINGS

The requirements and criteria for debriefing personnel who have had access to classified information are contained in paragraph 0108 of this instruction.

24 MAY 1961

EXHIBIT 2A

S - A - M - P - L - E

5520

Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (OP-09B31)

Subj: EMERGENCY APPOINTMENT TO A NONCRITICAL-SENSITIVE POSITION

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5510.60L

Encl: (1) Security Indoctrination Certification and Request for Clearance

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated noncritical-sensitive:

Full Name:
SSN:

DPOB:
Position/Job Title:

2. A National Agency Check and Inquiry/National Agency Check on (Name), (Grade), was submitted to the Office of Personnel Management/Defense Investigative Service on (Date). A request for security access is submitted as enclosure (1). It is requested that an Interim Secret clearance be granted per reference (b).

3. This exception is considered necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. (Name) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

OPNAVINST 5510.60L

24 MAY 1991

5. It is understood that Interim Secret clearance is automatically cancelled six (6) months from the date granted, upon granting final access, or upon transfer to duty outside (your division), whichever occurs sooner.

Copy to:
Cognizant Security Coordinator
S/HCPO (Code 39P)

24 MAR 1981

EXHIBIT 2B

S - A - M - P - L - E

5520
Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (OP-09B31)

Subj: EMERGENCY APPOINTMENT TO A CRITICAL-SENSITIVE POSITION

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5510.60L

Encl: (1) Security Indoctrination Certification and Request for Clearance

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated critical-sensitive:

Full Name:
SSN:

DPOB:
Position/Job Title:

2. A Background Investigation/Special Background Investigation on (Name), (Grade), was requested on (Date). A satisfactory NACI/NAC was completed on (Date) by the Office of Personnel Management/Civil Service Commission/Defense Investigative Service. A request for Security Access is submitted as enclosure (1). It is requested that an Interim Top Secret clearance be granted per reference (b).

3. This exception is considered necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. (Name) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

OPNAVINST 5510.60L

24 MAY 1991

5. It is understood that Interim Top Secret clearance is automatically cancelled six (6) months from the date granted, upon granting final access, or upon transfer to duty outside (your division), whichever occurs sooner.

Copy to:
Cognizant Security Coordinator
S/HCPO (Code 39P)

24 MAY 1991

EXHIBIT 2C

**PROCEDURES FOR CERTIFYING ACCESS TO
CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)**

1. Screening Procedures. Prior to certifying an individual for access to CNWDI, the following prerequisites must be verified:

a. The prospective recipient must have a valid DOD security clearance (Final Top Secret or Secret) based on the appropriate investigative requirements. (Chapter 21 of reference (a) applies.)

b. The prospective recipient must require access to nuclear weapons design information in the performance of his/her official duties. Strict adherence to the "Need-to-Know" principle must be observed.

2. Certification Procedures. The following procedures are to be followed when certifying an individual for access to CNWDI:

a. Verify the basic prerequisites outlined in paragraph 1 above.

b. Execute the personnel briefing form outlined in Exhibit 2D.

c. Execute the inter-office memo outlined in Exhibit 2E, ensuring that the appropriate certifying official's (outlined in Exhibit 2F) signature is annotated thereon. If the designated certifying official is not available, subordinates to the certifying official (if so authorized by the certifying official) may sign "for," "by direction," or "acting," as appropriate.

3. Update Procedures

a. Additions. Conduct screening, certification and submit inter-office memo in accordance with paragraphs 1 and 2 above.

b. Deletions. Provide copy of signed debriefing Certificate to OP-09B31.

24 MAY 1991

EXHIBIT 2D

BRIEFING/DEBRIEFING CERTIFICATE
CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION

PART I

1. I acknowledge that I have been authorized to receive or hold Critical Nuclear Weapons Design Information. I understand that the security of Critical Nuclear Weapons Design Information is of paramount importance and that unauthorized disclosure of such information will endanger the United States.

2. I understand that when I have a change in my assignment or duty which makes it no longer necessary for me to have access to Critical Nuclear Weapons Design Information, I must execute a Debriefing Certificate.

3. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, if I discuss with, or disclose Critical Nuclear Weapons Design Information to any person not currently authorized to have such information.

 (Date) (Signature) (SIGNATURE OF WITNESS) NAME (Printed or Typed)

=====

PART II

1. I acknowledge that I am no longer authorized access to Critical Nuclear Weapons Design Information. I certify that hereafter I will not divulge or discuss such information which I have acquired as an authorized recipient, unless required to do so by a competent authority.

2. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, for any unauthorized disclosure.

 (Date) (Signature) (SIGNATURE OF WITNESS) NAME (Printed or Typed)

24 MAY 1981

EXHIBIT 2E

S - A - M - P - L - E

5521
Date

From:

To: OP-09B31

Subj: CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION, CERTIFICATION
OF NEED-TO-KNOW

Ref: (a) DOD Directive 5210.2
(b) OPNAVINST 5510.60L

Encl: (1) Personnel certified for access to Critical Nuclear
Weapons Design Information

1. Per references (a) and (b), the personnel listed in enclosure
(1) are certified as having a need-to-know for Critical Nuclear
Weapons Design Information (CNWDI).

2. Briefing certificate(s) has/have been completed.

(Signed by Certifying Official)

24 MAY 1961

**PERSONNEL CERTIFIED FOR ACCESS TO
CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION**

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible, starting from the top edge and ending near the bottom edge. The lines are thin and black, providing a guide for writing or drawing.

24 MAY 1991

EXHIBIT 2F

LIST OF AUTHORIZED CNWDI CERTIFYING OFFICIALS

Secretary of the Navy
 Under Secretary of the Navy
 Assistant Secretary of the Navy (Research, Development & Acquisition)
 Assistant Secretary of the Navy (Manpower & Reserve Affairs)
 Administrative Aide to the Secretary of the Navy
 Director, Office of Program Appraisal
 Chief of Naval Operations (OP-00)
 Vice Chief of Naval Operations (OP-09)
 Assistant Vice Chief of Naval Operations (OP-09B)
 Director of Naval Intelligence (OP-092)
 Director of Navy Test & Evaluation & Technology Requirements (OP-091)
 Director, Test & Evaluation Division (OP-912)
 Deputy Chief of Naval Operations (Manpower, Personnel, and Training) (OP-01)
 Assistant Chief of Naval Operations (Undersea Warfare) (OP-02)
 Director, Strategic Submarine Division (OP-21)
 Assistant Chief of Naval Operations (Surface Warfare) (OP-03)
 Deputy Chief of Naval Operations (Logistics) (OP-04)
 Director, Materiel Division (OP-41)
 Assistant Chief of Naval Operations (Air Warfare) (OP-05)
 Deputy Chief of Naval Operations (Plans, Policy & Operations) (OP-06)
 Deputy Director, Strategic & Theater Nuclear Warfare Division (OP-65B)
 Head, Theater Nuclear Plans Policy & Requirements Branch, Strategic & Theater Nuclear Warfare Division (OP-653)
 Director, Antisubmarine Warfare Division (OP-71)
 Deputy Chief of Naval Operations (Navy Program Planning (OP-08)

24 MAR 1977

CHAPTER 3

CONTROL AND ISSUE OF BADGES AND PASSES

0301. DEPARTMENT OF DEFENSE BUILDING PASSES

1. Background. The Washington Headquarters Services/Physical Security Division is responsible for setting policies with regard to issuance of Department of Defense Building Passes. The OPNAV Security Branch has been assigned authority over applications for Department of Defense Building Passes for those individuals assigned to the Office of the Chief of Naval Operations, Immediate Offices of the Secretary of the Navy and the Department of the Navy Staff Offices.

2. Requirements for possession and use of Department of Defense Building Passes

a. Each individual, military or civilian, shall show his/her pass when entering the Pentagon Building. Additionally, DOD Building Passes must be displayed visibly on outer clothing at all times between 1800 and 0600 hours, Monday through Friday, all day on Saturdays, Sundays and holidays, or at the direction of the Director, Washington Headquarters Services. Building pass holders must exercise proper precautions to prevent loss of their passes. In the event a pass is lost, however, the loss must be reported immediately to the OPNAV Security Branch (OP-09B31). Administrative action may be taken by appropriate authorities in instances where the loss of the pass occurs due to:

- (1) Negligence,
- (2) Willful destruction or alteration,
- (3) Misuse, or
- (4) Occurs without the immediate notification of the OPNAV Security Branch.

b. If an individual has lost two passes through negligence, a third pass will not be issued until either one of the lost passes has been recovered or expires.

c. A final security clearance or favorably adjudicated investigation is required to issue a permanent building pass. A

24 MAY 1991

temporary pass may be issued for new employees when an investigation has been submitted but has not been completed.

d. The following forms are acceptable to enter the Pentagon between the hours of 0600-1800 Monday thru Friday:

- (1) DD Form 2 (Active Duty U.S. Military I.D. Card).
- (2) DD Form 2 (Retired U.S. Military I.D. Card).
- (3) DD Form 2N (Reserve U.S. Military I.D. Card).
- (4) DD Form 1173 (Uniformed Services and Privilege Card) except those cards marked "FM" or "FP" (Foreign Person) in block 11 on the lower left side.
- (5) DOD Civilian I.D. cards (DD Form, DA Form, AF Form, USN Form or those having a military return address) issued to active duty and retired DOD Civilian personnel containing the photograph and signature of the bearer.

Building passes will not be issued to those visitors with an identification card that qualifies under the above provisions except if assigned temporary additional duty (TAD), access is required after normal working hours and all requirements in subparagraphs 3b thru e are completed.

3. Procedures for Issue

a. Military and civilian employees. DOD Building Pass Requests (DD Form 2249) are issued from OP-09B31D, Room 4A662, Pentagon, for all military and civilian personnel permanently stationed or employed by the offices on distribution of this instruction.

b. Contractors

(1) Requests for DOD Building Passes for contractors will be considered on a case-by-case basis. Requests must be in writing, submitted to OP-09B31C by the Point of Contact (POC), and endorsed by the POC's Security Coordinator. Requests must also be accompanied by the original visit request (endorsed by OP-09B31C as outlined in Chapter 14 of this instruction.) Requests must also specify frequency of access required by the contractor, room number of the office to be visited, and briefly justify the need for a building pass. Approved requests will

24 MAR 1991

provide passes for the length of time specified on the accompanying visit request. The POC is responsible for notifying contractor(s) of approval/disapproval of building pass request, and for providing an escort to accompany the contractor during building pass processing. DOD Building Pass Requests (DD Form 2249) for contractors are issued from OP-09B31D in Room 4A662, Pentagon on Wednesdays only from 0800-1200.

(2) Requests for contractor building passes will only be approved if the issue of the pass will provide direct support or benefit to this command, not as a matter of convenience to the contractor. Concurrently, passes will not be issued to employees of contractor facilities not within commuting distance of the Pentagon Building, or to employees of contractor facilities who are under contract with another government agency in the National Capital Region (NCR), authorized to issue DOD Building Passes. Under no circumstances will NCR passes be issued to contractors.

c. Reserve Military Personnel

(1) Military personnel from permanent reserve units drilling within the Pentagon will be issued DOD Building Passes for the Pentagon based on a list provided from the Commanding Officer of their reserve unit certifying their clearance information to OP-09B31. Passes will not exceed a duration of one year. DOD Building Pass requests (DD Form 2249) are issued from OP-09B31D in Room 4A662, Pentagon.

(2) Military personnel assigned to the offices on distribution of this instruction and drilling for a short time-frame (usually 2 weeks) within the Pentagon, will be issued a temporary pass upon presentation of valid orders containing clearance information. DOD Building Pass requests (DD Form 2249) are issued from OP-09B31D in Room 4A662, Pentagon.

d. Military and Civilian employees visiting from other government commands

(1) Requests for DOD Building Passes for military and civilian personnel visiting offices listed on distribution of this instruction will be considered on a case-by-case basis. Requests must be in writing, submitted by the POC, and endorsed by the POC's Security Coordinator. Requests must also be accompanied by the original visit request (endorsed by OP-09B31D as outlined in Chapter 14 of this instruction). Requests must also specify frequency of access required by the visitor, room number of the office to be visited, and briefly justify the need for a

14 MAY 1991

building pass. Approved requests will provide passes for the length of time specified on the accompanying visit request. The POC is responsible for notifying visitor(s) of approval/disapproval of building pass request, and for providing an escort to accompany the visitor during building pass processing. DOD Building Pass Requests (DD Form 2249) for visitors are issued from OP-09B31D in Room 4A662, Pentagon.

(2) Requests for visitor building passes will only be approved if the issue of the pass will provide direct support or benefit to this command, not as a matter of convenience to the visitor. Concurrently, passes will not be issued to employees of other government commands not within commuting distance of the Pentagon Building unless visit request indicates the individual is temporarily assigned to an OPNAV/SECNAV office or to employees of government commands within the National Capitol Region (NCR) authorized to issue DOD Building Passes. Military personnel (active duty and retired) may use their military I.D. card to enter and exit the Pentagon Building during normal working hours (0600-1800). NCR passes will only be issued to visitors of those offices predetermined by OP-09B31 to justify such passes when requested by the POC.

e. All personnel reporting for processing of a DOD Building Pass must present a photographic I.D. (such as valid driver's license, other government agency or contractor facility I.D. card, expiring DOD Building Pass, military I.D. card or similar photographic I.D.) to be processed for a pass. Personnel escorting prospective pass recipients must remain with and are responsible for the prospective pass recipients until completion of pass issuance at the Building Pass Office.

0302. PROPERTY PASSES

1. Background

a. The removal of property from the Pentagon is governed by the Washington Headquarters Services/Physical Security Division. Regulations require that the authorized removal of government property not covered by a bill of lading or invoice shall be accomplished by means of a property pass.

b. Accountability for government property within the Office of the Chief of Naval Operations is under the cognizance of the Director, OPNAV Services and Security Division (OP-09B3) who is responsible to the Assistant Vice Chief of Naval Operations (OP-09B), for its accountability. Within the Offices of

24 MAY 1991

the Secretary of the Navy and the Department of the Navy Staff Offices, accountability for government property is under the cognizance of the Director, Secretariat Services and Support Division.

2. Procedures

a. Property Passes (GSA Optional Form 7) must be obtained during normal working hours. The Head, OPNAV Supply and Space Control Branch (OP-09B32), Room 5E577, the Director, Secretariat Services Support Division, Room 5E773, and their designated representatives are authorized to sign Property Passes for personnel desiring to remove items of government or private property.

b. After normal working hours, weekends, or holidays, Property Passes may be issued by the OPNAV Security Operations Center, Room 4A654. Passes will be issued when determined by the OPNAV Security Senior Watchstander that removal of personal or government property is in the best interest of the Navy and cannot be deferred until the next working day. Property bearing a CNO U.S. Government Property Tag (red in color) or a Chief of Naval Operations bar code label will not be released after hours.

0303. NAVAL DISTRICT WASHINGTON VEHICLE REGISTRATION PROCEDURES

1. Background

a. Per OPNAVINST 5560.10B and NDW INSTRUCTION 5560.2C (NOTAL), all eligible non-government-owned vehicles authorized to operate on board Department of Defense installations will be registered and marked.

b. The OPNAV Security Operations Center issues all non-government-owned vehicle registration stickers to Navy personnel permanently stationed or employed by the offices on distribution of this instruction and assigned to the Pentagon. Applications are available in the OPNAV Security Operations Center, Room 4A654.

2. Requirements

a. The following documents will be submitted for each vehicle to be registered:

(1) A completely filled out and signed "Automobile Registration Request," (HQ-NDW 5560/1).

24 MAY 1991

(2) The current certificate of state registration as evidence of ownership.

(3) If the applicant is not the owner of the vehicle, a written statement from the owner authorizing the applicant to use the vehicle.

(4) For motorcycle registration, proof of completion of the required motorcycle safety course.

(5) State driver's license.

(6) Proof of motor vehicle liability insurance in an amount not lower than the minimum limits prescribed by law of the state or jurisdiction in which the vehicle is registered by presentation of insurance policy or insurance carrier card.

24 MAY 1991

CHAPTER 4

CLASSIFICATION

0401. BASIC POLICY

1. Executive Order 12356 is the only basis for classifying information except as provided in the Atomic Energy Act of 1954, as amended. It is Department of the Navy policy to make available to the public as much information concerning its activities as possible, consistent with the need to protect national security. Therefore, information will be classified only to protect the national security.

2. Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, safeguard it as if it were classified at least "Confidential" pending a determination by an Original Classification Authority (OCA). When there is reasonable doubt about the appropriate level of classification, safeguard the information as if it were classified at the higher level until an OCA makes a determination. The OCA's determination must be made within thirty (30) days (see paragraph 6-12 of reference (a)).

0402. CLASSIFICATION DESIGNATIONS

1. Information which requires protection against unauthorized disclosure in the interest of national security must be classified with one of only three designations:

a. TOP SECRET. This designation is applied only to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples include armed hostilities against the U.S. or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

b. SECRET. This designation is applied only to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples include disruption of foreign relations significantly affecting the national security; significant impairment of a

24 MAR 1991

program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

c. CONFIDENTIAL. This designation is applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. Examples include information indicating strength of ground, air, and naval forces; performance characteristics, test data, design, and productions data on U.S. weapon systems and munitions.

2. The markings "For Official Use Only" and "Limited Official Use" cannot be used to identify classified information, nor can modifying terms be used in conjunction with authorized classification designations, such as "Secret Sensitive".

0403. FOR OFFICIAL USE ONLY (FOUO)

1. FOR OFFICIAL USE ONLY applies to information, records, and other materials which have not been given a security classification under the criteria of an Executive Order, but which contain information which may be withheld from the public for one or more of the reasons cited in Freedom of Information Act (FOIA) exemptions 2 through 9 (SECNAVINST 5720.42D). No other material shall be considered or marked FOR OFFICIAL USE ONLY (FOUO), as FOUO is not authorized as a form of classification to protect national security interests.

2. Paragraph 8 of SECNAVINST 5720.42D contains the guidelines for markings, dissemination, transmission and safeguarding FOUO information.

0404. ORIGINAL CLASSIFICATION AUTHORITY

1. The authority to originally classify information as Top Secret, Secret or Confidential rests with the Secretary of the Navy and his designees. The Secretary has designated the officials listed in Chapter 6, Exhibit 6A (Part I) of reference (a) as original Top Secret classification authorities. The authority to originally classify information as Secret or Confidential, as well, is inherent in this designation.

2. The Secretary has authorized CNO (OP-09N) to designate original Secret classification authorities. The officials delegated such authority are listed in Chapter 6, Exhibit 6A

24 MAY 1991

(Part II) of reference (a). Original Confidential classification authority is inherent in this designation.

3. Original Confidential classification authorities are not specifically designated. Original Confidential classification determinations will be made by original Top Secret and Secret classification authorities.

4. Only the incumbents of the positions listed in Chapter 6, Exhibit 6A of reference (a) have original classification authority and this authority is nondelegable. If an original classification authority is absent, however, the person designated to act in his/her absence may exercise the classification authority.

5. The OPNAV Security Manager (OP-09B31) maintains a current list of OPNAV/SECNAV/DON Staff Office officials designated as original Top Secret and Secret classification authorities, and ensures via CNO (OP-09N) that they are trained in their classification responsibilities. CNO (OP-09N) conducts an annual review of the continuing need for these officials to exercise the authority. To retain original classification authority, it must be exercised on the average of once every six months.

6. Submit requests for original classification authority to CNO (OP-09N) via the OPNAV Security Manager (OP-09B31). Each request must identify the nominee's position, title and organization and describe the circumstances in each of the areas contained in paragraph 6-3.6 of reference (a) that justify the delegation of such authority.

7. All original classification authorities must be indoctrinated in the fundamentals of security classification, limitations of their authority to classify and their responsibilities. The indoctrination is a prerequisite to granting original classification authority and shall be a matter of record subject to audit. CNO (OP-09N) has developed a program to ensure indoctrination of all current authorities and this program has been implemented by OP-09B31 for all original classification authorities under his cognizance. OP-09B31 will initiate the required action with personnel reporting aboard into a billet previously authorized as an original classification authority. The authority does not automatically carry forward with the newly reporting official until completion of the required indoctrination procedures.

24 MAY 1991

0405. ORIGINAL VS DERIVATIVE CLASSIFICATION

1. Original classification is the initial two-part determination that information requires, in the interest of national security, protection against unauthorized disclosure and a determination of the level of protection required. For example, a missile program manager determines that certain operational characteristics, such as speed, range and lethality, require classification at the Confidential level to ensure the missile's operational superiority throughout its life cycle. Those original classification determinations are issued as part of the program security classification guide. Subsequently, any time that information is used, by anyone in any form, it is derivatively classified Confidential based on that original classification determination.

2. Derivative classification can be accomplished by anyone who incorporates, paraphrases, restates, or generates in new form, information which is already classified. Derivative classification is most commonly accomplished by marking material per guidance from an original classification authority. An estimated 90 percent of the classified information produced by Department of the Navy commands is derivatively classified, i.e., based on a classified source document or a security classification guide. If it is believed that paraphrasing, restating, or summarizing of classified information has changed the level of, or removed the basis for classification, the cognizant original classification authority will be asked for a specific determination.

3. A derivative classifier must comply with the requirements contained in paragraphs 6-4.3 and 6-4.4 of reference (a).

4. Refer to Chapter 6 of reference (a) for detailed information regarding classification of information.

0406. INDUSTRIAL OPERATIONS

1. Industrial management does not make original classification determinations but applies the classification decisions of the government contracting authority. Classification in industrial operations under Department of the Navy contracting authority will be based strictly on security classification guidance furnished by the Department of the Navy. DOD 5220.22-M of March 1989 (NOTAL) requires contractors to apply the classification guidance accurately and uniformly to their operations.

24 MAY 1991

2. Navy and Marine Corps authorities are required by references (a) and (b) to use the DD Form 254, "Contract Security Classification Specification" to convey contractual security classification guidance to their contractors. A sample DD Form 254 is contained in Exhibit 15B. The appropriate security guides (promulgated by the 5513 series of OPNAV instructions) or other written narrative security classification guidance will be provided via the DD Form 254. Each DD Form 254 will be reviewed for currency and accuracy at least once every two years. Changes will conform with references (a), (b) and DOD 5220.22-M of March 1989 (NOTAL). All holders of the DD Form 254 will be provided any changes as soon as practicable. If there are no changes and the DD Form 254 remains current, all holders will be notified in writing to that effect.

24 MAY 1991

CHAPTER 5

MARKING

0501. BASIC POLICY

1. Classified material will be physically marked, annotated, or identified by other means, as prescribed in this chapter. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading and declassification actions. Therefore, all classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material.

2. Classified material is any product embodying classified information. Where the word "document" is used in this instruction, it means publications (bound or unbound, printed material such as military reports, studies, manuals), correspondence (such as military and business letters and memoranda), and other printed or written products (such as charts, maps). Most documents are easily marked, while other material such as hardware, recordings, photographs, etc., may be more difficult to identify because of physical characteristics. The markings in paragraph 0502, are required for all classified information, regardless of the medium by which it is revealed, with the following exceptions:

a. An article which has appeared, in whole or in part, in newspapers, magazines or elsewhere in the public domain, will not be marked, controlled or restricted in any manner, while it is being reviewed and evaluated for comparison with classified information. The results of the review and evaluation, if classified, must remain separate from the article in question.

b. Classified material will not be marked as prescribed in this chapter if the markings themselves would reveal a confidential source or relationship not otherwise evident in the material.

c. A declassification date or event, or the notation "Originating Agency's Determination Required" (OADR), will not be applied to material which contains, in whole or in part, Restricted Data (RD) or Formerly Restricted Data (FRD). RD and FRD

24 MAY 1991

information will not be declassified without the prior approval of the Department of Energy (DOE).

d. Classified correspondence to foreign governments or to their embassies, missions or similar official offices in the U.S., will be marked only with the overall classification. Copies of the correspondence held by the originating office and disseminated to other commands must carry all of the required markings.

0502. BASIC MARKING REQUIREMENTS

1. Marking requirements and the application of markings vary, depending on the kind of material. Basic markings required for all classified material are:

a. For originally classified material:

- authority. (1) The identity of the original classification (i.e., Position title and office code.)
- (2) The agency and office of origin.
- (3) The overall classification.
- (4) The declassification date or event or the notation, "Originating Agency's Determination Required" (OADR).
- (5) Any downgrading instructions.

b. For derivatively classified material:

- (1) The source of classification (e.g., source document or classification guide), including its date when necessary for positive identification. If you derive classification from more than one source, use the phrase, "Multiple Sources." Keep a listing of the multiple sources with the file or record copy of a document or the related or accompanying documentation for other kinds of classified material. (The listing is not distributed with the material.)
- (2) The agency and office of origin.
- (3) The overall classification.
- (4) The declassification date or event, or the notation, "Originating Agency's Determination Required" (OADR). If you derive classification from multiple sources, carry forward

24 MAY 1991

the most remote date or event for declassification marked on any of the sources. OADR is the most restrictive declassification instruction. If any source has this notation, you must use it instead of a declassification date.

(5) Any downgrading action required.

2. In addition to the foregoing, some material may require warning notices, intelligence control markings or distribution statements as described in paragraphs 9-32, 12-20 or Exhibit 12B of reference (a) respectively. Derivatively classified material will carry any warning notices or control markings from its sources that also apply to the new material.

3. Overall classification is the highest classification of any information contained in or revealed by the material. Overall markings are the overall classification, the most restrictive downgrading/declassification instructions applied to any information in the material and all warning notices or intelligence control markings applicable to the information in the material.

4. The classification authority, the office of origin, downgrading and declassification instructions, warning notices and intelligence control markings are collectively called associated markings.

5. Stamp, print or write classification markings in capital letters, larger than those used in the text of a document or conspicuously on other material, and, when practicable, colored red.

6. Classification and associated markings will be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal or similar device on classified materials other than documents, and on their containers. If the material or container cannot be marked, provide recipients with written notification of the classification and associated markings.

7. Mark major components of a document, which can be used independently, as individual documents. Examples are appendices and annexes to plans or operations orders. Enclosures to a letter of transmittal are always marked as individual documents. If an entire major component is unclassified, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included such as "All portions of this (annex, appendix, etc.) are UNCLASSIFIED". When

24 MAY 1991

this method is used, no further markings are required on the unclassified major component.

8. Chapter 9 of reference (a) contains detailed guidance for marking documents. Exhibits 9A through 9G of reference (a) are illustrations of markings. Exhibit 9H of reference (a) is a detailed marking guide for publications and correspondence. The text of the exhibits also provides amplification of marking requirements and should be read for additional guidance.

24 MAY 1991

CHAPTER 6

HANDCARRYING OF CLASSIFIED MATERIAL

0601. HANDCARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS

1. When classified material is being carried within the command or its immediate environs (your building) as part of normal duties, reasonable precautions, such as placing a cover-sheet over the material, will be taken to prevent inadvertent disclosure.

2. If the movement requires transportation other than walking, double-wrap and address the classified material. A briefcase may be considered the outer wrapping, except as noted in paragraph 0606.2a.

3. When classified material being carried is actually being transferred to another command, follow the requirements of Chapter 10 for wrapping, addressing, receipts, etc.

4. Contractor personnel are not authorized to handcarry classified material out of OPNAV/SECNAV/DON Staff Offices spaces. In urgent cases when delay in receipt of bids or delay of contracts would result, the project officer may request a waiver (with sufficient written justification), from OP-09B31. In every case, handcarrying by contractor personnel will only be permitted if it is to the advantage of the government. Each request will be handled individually by OP-09B31, must meet the requirements outlined in paragraph 1505, and a valid visit request meeting the requirements of paragraph 1403 with company courier authorization for the contractor must be on file in the requesting office and included with the request for waiver to OP-09B31.

0602. PROCEDURES FOR ACQUISITION AND USE OF COURIER AUTHORIZATION CARDS

1. Courier Authorization Cards (DD Form 2501) are for use by individuals handcarrying classified material by means of surface transportation within a commuting area of the command authorized by OP-09B31. Security Coordinators will submit requests for courier Authorization Cards to OP-09B31.

24 MAY 1991

2. OP-09B31 will review all requests for Courier Authorization Cards and issue cards when justified. Courier Authorization Cards will be released to the Security Coordinator only, not to the individual courier. Security Coordinators are responsible for maintaining accountability and control of Courier Authorization Cards issued to their custody. Security Coordinators may sub-custody control of Courier Authorization Cards to Assistant Security Coordinators under their cognizance. Courier Authorization Cards will be issued to individuals by the Security Coordinator (or Assistant Security Coordinator) on an "as needed" basis only and must be returned to the Security Coordinator upon completion of the courier trip. This means the Courier Authorization Card must be checked out from the Security Coordinator for each courier trip and turned in upon return of the courier. Individuals will not retain Courier Authorization Cards on a permanent basis to preclude unauthorized removal of classified material.

0603. AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS

1. Because of the security risk inherent in handcarrying classified material while in a travel status, the Assistant Vice Chief of Naval Operations (OP-09B) has delegated to the OPNAV Security Manager (OP-09B31), authority to authorize handcarrying when:

a. The classified material is required at the traveler's destination.

b. The classified material is not available at the command to be visited.

c. Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

NOTE: The Head, NATO Sub Registry/Top Secret Control Unit (OP-09B31C2) is the approval authority for handcarrying NATO materials as outlined in reference (d). For SCI material, approval must be obtained from the Director of Naval Intelligence (OP-092Z/SSO).

0604. PROTECTION DURING HANDCARRYING IN A TRAVEL STATUS

1. Personnel handcarrying classified material must be aware of the following:

24 MAR 61

a. The classified material must be in the individual's physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (continental U.S. only) is available. Handcarrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage in a government activity or a cleared facility. When any package containing classified material is surrendered for temporary storage (e.g. overnight or during meals), the individual must obtain a receipt signed by an authorized representative of the contractor facility or government installation accepting responsibility for safeguarding the package.

b. Classified material may not be read, studied, displayed, or used in any manner on a public conveyance or in a public place.

c. When the classified material is carried in a private, public, or government conveyance, it will not be stored in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank.

d. A list of all classified material carried or escorted by the individual will be maintained by his/her office; and upon his/her return, all classified material must be accounted for.

e. Whenever possible, the individual should return the classified material to his/her office by any one of the other approved methods of transmission as stated in reference (a). If material must be handcarried, approval and documentation must be obtained from command being visited.

0605. PROCEDURES FOR OBTAINING AUTHORIZATION TO ESCORT OR HANDCARRY CLASSIFIED MATERIAL ON COMMERCIAL PASSENGER AIRCRAFT

1. Because of the possibility of hijacking, classified material will be transported aboard commercial passenger aircraft only when other methods will not transmit the material in time to meet operational objectives or contract requirements.

2. The OPNAV Security Manager (OP-09B31), will approve handcarrying classified material aboard a commercial passenger aircraft upon receipt of a written statement authorizing the transmission signed by the cognizant Security Coordinator. This statement will include:

24 MAY 1991

- a. The reason the material cannot be transmitted by other means,
- b. If there are overnight stopovers, state plans for overnight storage of classified material, and
- c. Include an itemized list of material to be hand-carried.

In addition, the courier must have been issued a Courier Authorization Card (DD 2501), execute the Classified Couriers Responsibility Acknowledgment (Exhibit 6A) and you must prepare for signature by OP-09B31 an original letter on letterhead stationary authorizing the traveler to handcarry the material (Exhibit 6B). You must attach the addressed outer envelope or container so the OPNAV Security Manager can sign the outer container as required by Chapter 16 of reference (a). The letter must contain the information as shown in Exhibit 6B.

0606. PROCEDURES FOR CARRYING CLASSIFIED DOCUMENTS ABOARD COMMERCIAL AIRCRAFT

1. A traveler carrying classified documents aboard a commercial aircraft will process through the airline ticketing and boarding procedures in the same manner as all other passengers.

2. When traveling, you must:

a. Make sure the classified documents being carried have no metal bindings and are in double, sealed envelopes. (You may not consider a briefcase or luggage as the outer container in this circumstance.)

b. Present yourself at the screening station for routine processing. If you are carrying the documents in a briefcase or other carry-on luggage, the briefcase or luggage will be routinely offered for opening for inspection. The screening official will then be able to inspect the envelopes by flexing, feel, weight, etc., without any requirement for opening the envelopes themselves.

c. If the screening official is not satisfied, you will inform the official that the envelopes contain classified material, and you will then exhibit an official DOD pass or military I.D. card, plus your courier authorization. At that point, the screening official will process the envelopes with a detection device. If no alarm results, the envelopes require no

24 MAY 1991

further examination. If an alarm sounds and you are not permitted to board, contact the OPNAV Security Operations Center ((202) 695-3667 or 695-3121). The package is not to be opened under any circumstances as stated in your courier authorization letter.

3. See paragraph 16-7 of reference (a) for procedures for carrying classified material in packages aboard commercial passenger aircraft.

24 MAY 1991

EXHIBIT 6A

CLASSIFIED COURIERS RESPONSIBILITY ACKNOWLEDGMENT

The following is a list of responsibilities under OPNAVINST 5510.1H which apply to all authorized couriers of classified material:

1. Classified material must be in my physical possession at all times, unless under proper storage at a United States Government activity or an appropriately cleared contractor facility.
2. If necessary, overnight storage has been arranged with a government activity or cleared facility.
3. I will retain a receipt, signed by an authorized representative of the government activity or contractor facility, upon surrendering classified material for overnight storage.
4. When classified material is carried in a private, public or government conveyance, I will not store it in any detachable storage compartments such as automobile luggage racks, aircraft travel pods or drop tanks.
5. I may not read, study, display or use classified material in any manner on a public conveyance or in a public place, to include transportation inspection/screening personnel.
6. A complete detailed list of the contents of the material to be transported has been left with a designated authority in my activity.

I have read, fully acknowledge and understand my responsibilities as an authorized courier of classified material.

(DATE)

(SIGNATURE)

24 MAY 1991

EXHIBIT 6B

From: Chief of Naval Operations
To: To Whom It May Concern

Subj: COURIER AUTHORIZATION

1. Mr. John Thomas Doe (full name) of Chief of Naval Operations (name of activity) is authorized to handcarry three sealed packages, 9" x 8" x 24" (describe package(s) being carried) from Chief of Naval Operations, Pentagon, Washington, DC (addresser) to U.S. Naval Postgraduate School, Monterey, CA (addressee name) on 14 June 1989 (date).
2. Flight #59 departs National Airport at 1100 and arrives at (insert flight information including transfer points) Los Angeles International Airport at 1400.
3. Mr. John Thomas Doe (name of courier) will carry a DOD Badge #12345 (type of I.D. w/photo.) (If the courier is a civilian, include height, weight, date of birth and signature.)
4. This authorization expires 0900/07 June 1989 (Time/date not to exceed 7 days from date of issue.)
5. Confirmation of this authorization may be obtained by calling (202) 695-3667 or autovon 225-3667.
6. This package contains classified material and is not to be opened under any circumstances.

JERRY C. BARNHARDT
Director, Security Programs/
Command Security Manager

Copy to:
OP-09B31D

24 MAY 1991

CHAPTER 7

ACCOUNTING AND CONTROL

0701. BASIC POLICY

1. Classified information must be afforded a level of accounting and control commensurate with its assigned classification. Accounting and control serves to: limit dissemination; prevent unnecessary reproduction; determine the office or person normally responsible for the material's security; and determine holders so they can be notified of unscheduled changes in the classification or compromise of the material. In the case of Top Secret information, it is also important to keep a current record of who has the information and who has seen it.

2. Common sense dictates that absolute accountability and control cannot be provided for all classified information. It is therefore necessary, to make distinctions in the degree of accountability and control and to set standards commensurate with the degree of damage to the national security which might result from unauthorized disclosure of Top Secret, Secret or Confidential information.

3. Each ACNO, DCNO, DSO, ASN and Director of DON Staff Office must establish screening points to ensure that all incoming mail and material delivered to offices under their cognizance is adequately protected until a determination is made as to whether it contains classified material. If incoming mail or material delivered to an office has not been screened and a determination made as to whether it contains classified material or not, then the material may not be left unattended. This material must be secured in a security container when unattended until the determination is made.

0702. TOP SECRET

1. The designated directorate Top Secret Control Officer (TSCO), is responsible for receiving, maintaining accountability, distributing, reproducing and the destruction all Top Secret Material for his/her directorate. Top Secret accountability and control procedures will be included in each directorate's internal security instruction.

2. All Top Secret documents originated or received must be turned over to their directorate TSCO and entered into the

24 MAY 1991

accountability register. The register will completely identify the Top Secret document including changes, show the number of copies and give the disposition of each copy. The register will be retained for five years after the documents are transferred, downgraded or destroyed.

3. Each directorate TSCO shall serially number all copies of each Top Secret document and each item of Top Secret equipment at the time of origination in the following manner:

"Copy no. __ of __ copies."

Exceptions to this rule are allowed for publications containing a distribution list by copy number and for mass produced reproductions when costs of serially numbering would be prohibitive. In the latter case, adequate and readily available documentation must be maintained indicating the total number of copies produced and the recipients of the copies. Copy numbers may be applied to Top Secret microfilm by the use of adhesive stickers, adhesive stripping on headers, pin punching or marking pins.

4. If more than one microform is required in the micro-reduction of a Top Secret document or group of documents, indicate the number of microforms used. There is, at this time, no standardized technique for reflecting the number of microforms used. Any local technique which accurately reflects the number of microforms is acceptable. For Top Secret microfiche, indicate the data in the lower right portion of the header.

5. Top Secret documents will contain a list of effective pages in which will be included a Record of Page Checks. When this is impractical, as in correspondence or messages, number the pages as follows:

"Page __ of __ pages."

6. The directorate TSCO will page check Top Secret documents for completeness and accuracy on initial receipt and after entry of a change involving page entry or removal. This page check will be annotated on the Record of Disclosure and include the printed or typed name and signature of the individual performing the page check and date accomplished. (The change residue, including pages removed, must also be page-checked before destruction.) Page checks by the relieving officer, upon relief of a directorate TSCO as custodian, are not required unless specifically directed.

24 MAY 1991

7. Top Secret documents will be physically sighted, or accounted for by examination of written evidence of proper disposition, such as certificate of destruction, transfer receipt, etc., at least once annually, and more frequently when circumstances warrant. At the same time, audit Top Secret records to determine completeness and accuracy. Procedures for Top Secret audit and inventory are exhibit 7A.

8. Retention of Top Secret documents will be kept to a minimum. Return Top Secret documents to the directorate TSCO for destruction as soon as their intended purpose has been served. When Top Secret is destroyed, prepare a record of destruction identifying the material destroyed and the two officials who witnessed its destruction. Reevaluate Top Secret documents which cannot be destroyed and, when appropriate, downgrade, declassify, or retire them to designated records centers.

9. Account for Top Secret material by a continuous chain of receipts. Hand to hand transfer with signed receipts is required for internal distribution of Top Secret, with a record kept of each individual to whom the information is disclosed. Return Top Secret Material to the directorate TSCO for transfer outside of your directorate or command.

10. The directorate TSCO will maintain a disclosure record for each Top Secret document which shows the document title, printed or typed name and signature of all individuals, including stenographic and clerical personnel, who have been afforded access to the document and the date of access. Those in the directorate who may have access to containers in which Top Secret information is stored, or who regularly administratively handle a large volume of Top Secret information need not be included in disclosure records. They would be identifiable by roster as having had access on any given date. The directorate TSCO shall retain disclosure records (OPNAV 5511/13, Exhibit 7B) and applicable rosters of administrative personnel for two years after the documents are transferred, downgraded, or destroyed.

11. Top Secret material will only be reproduced by the directorate TSCO and may not be reproduced without the consent of the originating agency or higher authority. Authority to reproduce will be obtained by the individual requiring the reproduction and forwarded with the Top Secret document to their directorate TSCO for action. Annotate serially each copy produced.

24 MAY 1991

0703. SECRET

1. Within internal directorate security instructions, administrative procedures shall be established for controlling Secret material to include records of material (a) originated or received by the directorate; (b) distributed or routed to divisions or branches within the directorate; and (c) disposed of by the directorate by transfer of custody or destruction. The record may be a mail log, a communications log, file of route slips, serial file or other administrative record. (See Exhibit 10C pf reference (a) for sample accounting systems.)

2. Signed receipts are not required for Secret material distributed or routed within the directorate. Receipts are required when Secret material accountability will be transferred from one Classified Material Control Center (directorate) to another, whether or not within the command. Little security is added by requiring that a recipient in the office, department or division sign for this material. The person who signs is usually an administrative medium and is not the one for whom the material is intended.

3. Directorate heads may require additional controls for Secret material if he/she feels they are necessary and they represent a practical balance of security and operational efficiency.

4. When transmitting Secret material, enclose a receipt identifying the document(s). This receipt must be signed and returned to the sender regardless of the method of transmission. The Registered Mail receipt does not replace the Secret receipt. A Registered Mail receipt merely acknowledges that a package was received; it doesn't assure the sender that each piece of Secret material has been entered into the accountability system of the recipient. The sending command is responsible for material until the addressee receives it. The sender cannot be sure that accountability has been transferred until the recipient signs the receipt and returns it.

5. This command is not required to enter SECRET message traffic received through the Telecommunications Center into accountability and control records. To safeguard messages, protect them appropriate to their level of classification; control internal routing through "need-to-know" and reproduce SECRET messages only per the requirements outlined in paragraph 0801.

24 MAY 1981

6. Secret destruction must be recorded, but separate certificates do not have to be prepared, nor does destruction have to be centralized. The medium in which receipt was recorded may also be used to record the destruction. Two witnesses to the destruction of Secret material are required (see paragraphs 1202 and 1203).

0704. CONFIDENTIAL

Procedures for protection of Confidential information are less stringent than those for Secret. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. Administrative provisions are required, however, to protect Confidential information from unauthorized disclosure by access control and compliance with the regulations on marking, storage, transmission and destruction.

0705. WORKING PAPERS

1. Working papers are documents and material (including drafts, photographs, etc.), accumulated or created while preparing finished material. When working papers contain classified information, the accounting and marking requirements prescribed for the classification may be modified. As a minimum, working papers containing classified information will be:

- a. Dated when created.
- b. Marked on each page with the highest classification of any information they contain.
- c. Protected under the provisions of the classification assigned.
- d. Destroyed, by authorized means, when no longer needed.

2. Follow the accounting, control and marking requirements prescribed for a finished document however, when working papers contain TOP SECRET information or are:

- a. Released by the originator outside of the command, transmitted electrically or transmitted through message center channels within the command.
- b. Retained more than 90 days from date of origin.

24 MAY 1991

c. Placed permanently in a file system.

3. Classified notes from training courses or conferences are considered working papers, with the same conditions imposed as paragraphs 1 and 2 above.

NOTE: The downgrading/declassification statement will be placed on working papers when they are created if it is known at the time. This precludes the author having to research what his/her source(s) of classification used were, if necessary for permanent files.

0706. OTHER REQUIREMENTS

Additional accounting and control requirements for special categories of classified material are contained in the following directives:

1. COMSEC material - Cryptographic Security Policy and Procedures, CSP-1 (NOTAL), and Communications Material Systems Manual (CMS-4) (NOTAL).

2. NATO classified material - OPNAVINST C5510.101D and OPNAVINST 5510.100B (reference (d)).

3. Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI) - OPNAVINST S5511.35J (NOTAL).

24 MAY 1991

EXHIBIT 7A

TOP SECRET AUDIT AND INVENTORY

1. An inventory of all Top Secret material will be conducted at change of directorate TSCO, and at least once annually. Annual report is due on 15 February each year. Change of directorate TSCO inventory report is due with the appointment notice to OP-09B31. (For change of directorate TSCO, relieving directorate TSCO will conduct the inventory.) At the same time, the Top Secret records are to be audited to determine completeness and accuracy. Publications distributed under the Communications Security Material System will be sighted and accounted for per CMS-4. The inventory listing must include the following for each item: control number, any other internal control number assigned, copy number, originator, serial number, date, document title and/or subject (if unclassified).

2. Preliminary to conducting an inventory of Top Secret material, audit the records as follows:

a. Use the last inventory of holdings determined by the previous audit.

b. Add all incoming and outgoing material since that inventory, as indicated by higher sequence control log sheets.

c. Delete the material transferred or destroyed since the last audit as determined by records of destruction, receipts, or completed control log sheets.

d. List the remaining documents as the audit Top Secret material accountable (for inventory) by the command.

3. The directorate TSCO will provide any divisional ATSCOs with a list of their holdings (see page 7A-2 of this exhibit). The divisional ATSCOs will inventory the material held and report the results to the directorate TSCO by memorandum. (See page 7A-2 of this exhibit.)

4. Inventory all Top Secret material listed in the current audit by physically sighting each document on the directorate inventories. The directorate TSCO will report the results of the inventory by memo to the OPNAV Security Manager. (See page 7A-3 of this exhibit.)

OPNAVINST 5510.60L

24 MAY 1991

EXHIBIT 7A

TOP SECRET AUDIT AND INVENTORY

5511
Date

MEMORANDUM

From: Directorate Top Secret Control Officer
To: (Divisional) Assistant Top Secret Control Officer
Subj: DIRECTORATE TOP SECRET INVENTORY
Ref: (a) OPNAVINST 5510.60L
Encl: (1) Listing of Top Secret Holdings

1. According to my records, you have custody of the Top Secret documents listed in enclosure (1). Please conduct an inventory per reference (a) and report results by endorsement.

(Signature and date)

24 MAY 1991

5511

Date

MEMORANDUM

From: (Divisional) Assistant Top Secret Control Officer
To: Directorate Top Secret Control Officer

Encl: (1) Listing of Top Secret Holdings

1. I have inventoried and physically sighted the Top Secret documents listed on enclosure (1) in my custody.
2. The following discrepancies exist:

(Signature and date)

OPNAVINST 5510.60L

24 MAY 1991

EXHIBIT 7A

TOP SECRET AUDIT AND INVENTORY

5511

Date

MEMORANDUM

From: Directorate Top Secret Control Officer
To: OPNAV Security Manager (OP-09B31)

Subj: DIRECTORATE TOP SECRET INVENTORY

Ref: (a) OPNAVINST 5510.60L

Encl: (1) Top Secret Inventory Listing

1. I have inventoried all documents listed on the audit report of (date) (enclosure (1)).
2. The following discrepancies exist:

(Signature and date)

RECORD OF DISCLOSURE OPNAV 5511.13 (REV. 1-76) S/N 0107-17-0551105 U.S. Government Printing Office 1976-682-076-0002		TOP SECRET (Unclassified when detached from document)	
ACTIVITY Chief of Naval Operations (OP-097)		APPLICABLE CONTROL NO. T-567-86	
ORIGINATOR Chief of Naval Operations (OP-099)		CNO - NO 2	SERIAL NO. 6T123456
<p>The attached material contains TOP SECRET information which bears directly upon the effectiveness of our national defense or the conduct of foreign relations. In case of an emergency, unauthorized disclosure can reasonably be expected to cause a potentially grave damage to the national security. As such, the attached material derives special care in its handling, custody, and storage as required by the Department of the Navy Information Security Regulations, OPNAV Instruction 5510.1. This form is to be used as a record of persons who have read or had access to them all or any part of the TOP SECRET information contained in the material identified above. This form is NOT A R111P1.</p>			

Revised below each person who gets transmits has custody of, or otherwise obtains knowledge of the TOP SECRET contents of the attached material (b) NOT TO TRANSMIT this Revised of Disclosure unless the material is to be transmitted to another entity for retention

[illegible]

TOP SECRET (Unclassified when detached from document)

24 MAY 1991

CHAPTER 8

PRINTING, REPRODUCTION AND PHOTOGRAPHY

0801. CONTROLS ON REPRODUCTION

1. Because there are so many reproduction machines throughout OPNAV/SECNAV/DON Staff Offices spaces, the problems associated with reproducing classified material have continued to grow. The convenience of reproduction equipment does not preclude obtaining the proper authorization needed for reproducing classified material.

2. Top Secret information must not be reproduced without the consent of the originating activity or higher authority obtained and forwarded to your directorate TSCO. All reproduction of Top Secret Material will be accomplished by the cognizant directorate TSCO only.

3. ACNOs, DCNOs, DSOs, ASNs and Directors of DON Staff Offices must designate officials who will approve all requests to reproduce Secret material. These officials in turn have the responsibility to ensure that all reproduction prohibitions are observed and that the reproduction of classified material is kept to an absolute minimum. Personnel within all divisions must be made aware of the requirement for approval of one of these designated officials before reproducing classified material. It is suggested that these designated officials be Security Coordinators.

4. Records will be maintained to show the number and distribution of all reproductions of Top Secret documents, classified documents covered by special access programs distributed outside the originating agency, and Secret and Confidential documents marked with special dissemination and reproduction limitations.

5. Specifically designate the reproduction equipment authorized for reproducing classified material and prominently display signs on or near the equipment, advising users. Signs are available in the OPNAV Security Office (OP-09B31). Reproduction machines should be located within areas that are easily observed to ensure that only authorized copies are being made and the number of copies is kept to a minimum. Only equipment under the control and use of the directorate TSCO will be authorized for the reproduction of Top Secret Material.

24 MAY 1991

6. If the designated equipment involves reproduction processes using extremely sensitive reproduction paper, the paper will be used and stored in a manner to preclude image transfer of classified information.

7. Apply the same security controls to reproduced copies of classified documents as the originals require.

8. Reproduced material must show the classification and other special markings which appear on the original material from which copied. Double check all reproduced material and remark the reproduced copies on which the markings are unclear.

9. Safeguard any samples, waste or overruns resulting from the reproduction process, according to the classification of the information involved. Destroy this material promptly as classified waste. Check areas surrounding reproduction equipment for classified material that may have been left on nearby desks or thrown in wastebaskets. In the event the machine malfunctions, check to ensure that all copies have been removed. After reproducing classified material, make sure the original and all copies have been removed from the machine.

10. Reproduced copies of classified documents made with typical office copiers can leave legible images on the plastic surfaces of many three-ring and similar binders. The image transfers to the binder after the paper and plastic are in contact for some time. Classified document cover sheets should be used to preclude transferring the classified image to the cover of plastic binders.

0802. TELECOPIERS

Telecopiers, facsimile equipment or similar devices using non-secure telephone lines will not be used to transmit classified information.

24 MAY 1981

CHAPTER 9

DISSEMINATION OF CLASSIFIED MATERIAL

0901. BASIC POLICY

1. ACNOs, DCNOs, DSOs, ASNs and Directors of DON Staff Offices will establish procedures for disseminating classified material originated or received by their offices, to limit outside dissemination to those activities having a "need-to-know" and to reflect any restrictions imposed by originators or higher authority. Procedures will be issued as a part of the internal instruction required by Chapter 1 and will include, but not be limited to:

a. As a minimum, an annual review of classified material distribution lists to ensure classified material is disseminated on a strict "need-to-know" basis, and

b. Request removal from distribution of unneeded classified material received.

3. ACNOs, DCNOs, DSOs, ASNs and Directors of DON Staff Offices will ensure that material prepared for public release does not contain classified information or proscribed technical data. (See paragraph 12-25 of reference (a) for dissemination of technical documents.) Policies and procedures governing public release of official information and the circumstances under which security review is required are detailed in SECNAVINST 5720.44A (NOTAL). Certain categories of information require review and clearance by the Assistant Secretary of Defense (Public Affairs), and are listed as Exhibit 12A of reference (a). These categories of information are processed for public release under the procedures described in SECNAVINST 5720.44A (NOTAL). (See paragraph 12-15 of reference (a) for release of information to the Congress.)

0902. NATO MATERIAL

See OPNAVINST C5510.101D (NOTAL) and reference (d), for guidance on dissemination of NATO information. DON documents incorporating NATO information and marked according to paragraph 9-24 of reference (a) do not require transmission through NATO channels.

24 MAY 1991

0903. TOP SECRET MATERIAL

Top Secret material originated within the DOD will not be disseminated outside the DOD without the written consent of the originating department or agency, or higher authority. Provide this written consent to the cognizant directorate TSCO when requesting dissemination.

0904. SECRET AND CONFIDENTIAL MATERIAL

Secret or Confidential material originated within the DOD may be disseminated to other departments and agencies of the Executive Branch of the Government unless specifically prohibited by the originator.

0905. DISSEMINATION TO DOD CONTRACTORS

Information regarding the dissemination of classified material to DOD contractors is contained in Chapter 15.

0906. DISCLOSURE TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS

Information regarding disclosure to foreign governments and international organizations is contained in paragraph 12-14 of reference (a).

0907. DISSEMINATION TO CONGRESS

Information regarding disclosure to congress is contained in paragraph 12-15 of reference (a).

0908. GENERAL POLICY FOR DISSEMINATION OF INTELLIGENCE

1. Authorized channels for dissemination of intelligence are the departments and agencies which comprise the Intelligence Community as delineated in Executive Order 12333, Intelligence Community contractors and consultants and, within each department or agency, those channels designated by its Senior Official of the Intelligence Community (SOIC). Other channels for dissemination may be specified by the Director of Central Intelligence, in consultation with the National Foreign Intelligence Board (NFIB) or as agreed to between the originating and recipient agencies. The Intelligence Community includes: Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; special offices within the Department of Defense for the collection of specialized foreign intelligence through reconnaissance

24 MAY 1991

programs; the Bureau of Intelligence and Research of the Department of State; the intelligence elements of the military services; the Federal Bureau of Investigation; the Departments of Treasury and Energy; the Drug Enforcement Administration; and staff elements of the office of Director of Central Intelligence. The Director of Naval Intelligence (OP-092) is the Department of the Navy's SOIC.

2. The term intelligence means foreign intelligence and counterintelligence and information describing U.S. foreign intelligence and counterintelligence activities, sources or methods, equipment, and methodology used for the acquisition, processing, or exploitation of intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. intelligence collection efforts.

3. Any office desiring to disseminate intelligence requiring prior authorization by the originator, or in a manner contrary to the restrictions prescribed by the control markings in paragraph 12-20 of reference (a), must request permission from the originator via Chief of Naval Operations (OP-092). Permission granted applies only to the specific purposes agreed to by the originator and does not automatically apply to any other recipient. Originators must give prompt consideration to these requests, particularly to reviewing, and editing if necessary, sanitized or paraphrased versions to derive a text suitable for release with lesser or no control markings.

4. Department of Defense contractors may be provided selected intelligence when required in the performance of a Department of the Navy contract unless specifically prohibited by paragraph 0911. Intelligence will be released on a strict "need-to-know" basis. Authorization for release of intelligence to a contractor in the performance of a specific contract in no way implies authorization for release under another contract. Each release is treated separately, and authorization is required in each specific case, including release of revised editions of publications initially released. Commander, Naval Intelligence Command (NIC-52) is responsible for execution of the policies on release of intelligence to contractors and is the final authority for determinations requiring refusal (see paragraphs 0909, 0910 and 0911).

5. Violations of the restrictions and control markings prescribed in this instruction and reference (a) that result in

24 MAY 1991

unauthorized disclosure by one agency of the intelligence information of another, to which a DON command is a party, is to be reported to CNO (OP-09N).

0909. PROCEDURES FOR THE RELEASE OF INTELLIGENCE TO CONTRACTORS

1. When necessary for the performance of a DON contract, commands may release intelligence to DOD contractors without approval of Commander, Naval Intelligence Command.

2. Prior to releasing intelligence to a contractor, the releasing office will:

a. Ensure that dissemination is not prohibited by paragraph 0911.

b. Ensure that the conditions of paragraph 0910 are met prior to release.

c. Ensure that all parts of the intelligence being released fall within the scope of the contract under which requested. When all parts are not releasable, the releasing office will sanitize the intelligence information. (See paragraph 0910 below for sanitization procedures.)

3. The releasing office must maintain a record of all intelligence information released to contractors and report releases to the originator upon request.

4. Contracting officers will ensure that the requirements outlined in Chapter 15 are specifically included in the contract itself or in the Contract Security Classification Specification (DD Form 254).

0910. SANITIZATION

The office releasing intelligence to a contractor is responsible for proper sanitization. If the releasing office is not aware of specific contractual commitments, coordinate release of the intelligence information to be released with those activities which are able to determine the scope of the contract and "need-to-know" requirements of the contractor. Sanitization procedures for Central Intelligence Agency documents will always include the deletion, from all CIA Directorate of Operations reports, of the CIA seal, the phrase "Directorate of Operations," the place acquired, the field number, the source description, and field dissemination, unless prior approval to release that information

24 MAY 1991

is obtained from CIA. Forward any requests for approval via Commander, Naval Intelligence Command (NIC-52).

0911. PROHIBITED RELEASE

1. The following intelligence materials will not be released to contractors:

- a. National Intelligence Estimates (NIEs).
- b. Special National Intelligence Estimates (SNIEs).
- c. National Intelligence Analytical Memoranda.
- d. Interagency Intelligence Memoranda.
- e. DIA Fact Book.

2. The following intelligence materials will not be released to contractors without approval of the originator, obtained through the Commander, Naval Intelligence Command (NIC-52):

- a. Material which bears the following markings:

- (1) NOT RELEASABLE TO CONTRACTORS/CONSULTANTS
(NOCONTRACT)

- (2) CAUTION PROPRIETARY INFORMATION INVOLVED (PROPIN)

- (3) DISSEMINATION AND EXTRACTION OF INFORMATION
CONTROLLED BY ORIGINATOR (ORCON)

- b. Intelligence from Foreign Service reporting.

- c. Intelligence materials which are marked for special handling in special dissemination channels (sensitive compartmented information (SCI)).

3. Requests for authority to release material in the categories listed in paragraph 2 above will be addressed to the Commander, Naval Intelligence Command (NIC-52), via the command sponsoring the contract for validation of "need-to-know", and include the following information:

- a. Name of the DON contractor for whom the intelligence is intended.

24 MAY 1991

- b. Contract number on which the request is predicated.
- c. Sponsoring contracting officer's command.
- d. Certification of contractor's facility clearance and storage capability for safeguarding classified material.
- e. Complete identification of the material for which a release determination is desired.
- f. Statement of justification confirming "need-to-know" and containing a concise description of that portion of the contractor's study or project which will confirm the "need-to-know" for the intelligence information requested. This statement is a prerequisite for a release determination.

0912. AUTHORIZED SPECIAL MARKINGS WITHIN OPNAV STAFF

1. Where an originating or routing office requires more restrictive dissemination of classified or other correspondence, within OPNAV, than would be indicated by normal markings under reference (a), the special marking authorized in this paragraph shall be used in addition to, but not as part of, the prescribed classification marking. The authorized special marking is "CONTROLLED OPNAV CORRESPONDENCE -- CATEGORY (fill in category number)." The authorized special marking categories are as follows, with the most restrictive designated as Category I:

a. Category I. This document is to be read by specified addressee only. Further distribution or reproduction must be approved by the originator or superior authority.

b. Category II. Reproduction of this document is prohibited without approval of originator or superior authority. Distribution is limited to addressees and their immediate staffs only.

c. Category III. This is a working or other type of internal correspondence document, no portions of which are authorized for release outside OPNAV without approval of the originator or superior authority.

2. The appropriate special marking will be applied at the top of each page, on the envelope, and on the cover or routing sheet, when papers are originated and being "staffed" within OPNAV. When the originator or superior authority determines that the original reasons for assigning the special markings are no

24 MAY 1991

longer valid, the special markings will be removed from the correspondence or obliterated.

3. Copies of categories I and II will be marked in RED ink "Copy _____ of _____ Copies" to aid in accountability.

4. When highly sensitive correspondence originated external to OPNAV is given distribution within OPNAV, this may be given a special marking during the period it is in routing. In these instances, a cover page, marked with the appropriate special marking will be attached to the correspondence. In addition, the title of the correspondence with the originator and a chop list will be shown. Dissemination will be restricted per this chop list and the special category assigned. When in routing or not in use, category I and category II correspondence will be retained in a sealed envelope showing the special category assigned, the originating/routing office and the next addressee. After distribution is completed, the original correspondence and the chop list will be retained by the controlling OP-Code in a sealed envelope until destruction of the original is appropriate. The chop list will be retained for two years after destruction of the original.

0913. LIMITED DISSEMINATION CONTROLS (LIMDIS)

1. Limited Dissemination (LIMDIS) control to restrict need-to-know access to certain National Security Information (NSI) within the DON has been authorized as an additional need-to-know protective measure for safeguarding NSI when a Special Access Program (SAP) is not appropriate.

2. Designated Top Secret Original Classification Authorities (OCAs) may initiate formal LIMDIS measures for classified NSI under their functional cognizance after approval by CNO (OP-09N2). LIMDIS controls are less stringent and are administered differently than the procedures for a Special Access Program (SAP). Approved LIMDIS controls will be imposed only inside the DON unless expressly coordinated via the CNO (OP-09N2) for application by agencies outside the DON.

3. LIMDIS controls established by Top Secret OCAs will conform with the terms and conditions prescribed in Exhibit 9A, and use an approved LIMDIS control nickname assigned by CNO (OP-09N2). Exhibit 9B provides a sample LIMDIS briefing acknowledgement that will be adapted by Top Secret OCAs; no other type of non-disclosure statement is authorized.

24 MAY 1991

EXHIBIT 9A

CRITERIA FOR TOP SECRET ORIGINAL CLASSIFICATION
AUTHORITIES TO ESTABLISH LIMDIS CONTROLS

1. Limited Dissemination (LIMDIS) controls are approved by the Chief of Naval Operations (OP-09N2) and may be established for specified time periods by a Department of the Navy (Department) Top Secret Original Classification Authority (OCA) for clearly-defined National Security Information under the cognizance of that OCA or a subordinate in the chain of command, for application only within the Department.
2. Security classification guides for the LIMDIS information shall be developed as required by reference (a) and OPNAVINST 5513.1D.
3. Instructions governing LIMDIS controls shall emphasize the need-to-know protective measures available within the regular security system, and shall not confuse LIMDIS controls with those more restrictive measures imposed for a Special Access Program as described in SECNAVINST S5460.3A (NOTAL) and OPNAVINST S5460.4C (NOTAL).
4. All Department LIMDIS control information shall be assigned an unclassified nickname approved by the CNO (OP-09N2). Code words are not authorized for LIMDIS information.
5. LIMDIS control information shall be clearly marked with the approved nickname.
6. Navy commands originating or dealing with LIMDIS information will identify their personnel who are authorized local access. Centralized access control is not authorized, but lists of authorized personnel may be maintained locally. The cognizant Top Secret OCA or the CNO (OP-09N2) may direct that such lists be forwarded in special circumstances, as when compiling a complete historical record of access or for legal or oversight purposes.
7. Briefings as shown in Exhibit 9B will be provided to local personnel concerning the LIMDIS controls and access limitations. Records of such briefings will be maintained locally for two years after termination of the member's access. Specifically prohibited are unique security requirements such as LIMDIS control nondisclosure statements.

24 MAY 1991

8. Additional physical security restrictions will not be imposed except to require placing the LIMDIS material in sealed envelopes within approved storage containers to avoid inadvertent disclosure or mingling with other files.

9. Inner envelopes containing LIMDIS information or data will be marked "TO BE OPENED ONLY BY PERSONNEL AUTHORIZED LIMDIS (NICKNAME) ACCESS."

10. Electrically transmitted messages carrying LIMDIS information or data will be marked with the caveat LIMDIS (Nickname).

11. Under no circumstances will terminology be used indicating enhancements to need-to-know such as "Special Need-to-Know (SNTK)," "MUST KNOW," "Controlled Need-To-Know (CNTK)," or other similar bogus security upgrade designations.

12. CNO (OP-09N2) will prescribe unique oversight procedures to be conducted by professional security personnel which will ensure that LIMDIS controls are initiated and continued only so long as they are essential to provide the additional security.

13. LIMDIS controls will be reviewed to determine their continued need during the biennial review of the security classification guide as required by OPNAVINST 5513.1D.

24 MAY 1991

EXHIBIT 9B

SAMPLE LIMITED DISSEMINATION BRIEFING ACKNOWLEDGEMENT

Name:

Activity:

Social Security Number: (See PA Notice) Telephone No.:

CERTIFICATION BY BRIEFING OFFICIAL(*)

I certify that the person identified above meets the security clearance and need-to-know requirements for access to the classified national security information defined below, and that he/she has been briefed on the Limited Dissemination (LIMDIS) control protective measures which apply to this information.

ACKNOWLEDGEMENT OF MEMBER BRIEFED(**)

Access to information requiring LIMDIS control measures:

NICKNAME: LIMIT (Second word approved by the CNO (OP-09N2))

DEFINITION: (As approved by the CNO (OP-09N2))

1. I acknowledge that I have been briefed concerning the LIMDIS control measures identified and defined above. I further acknowledge that I understand the reason for these formal measures in applying the need-to-know principle for classified information as authorized by a Department of the Navy Top Secret Original Classification Authority.

2. I understand that LIMIT (*****) information I receive is given only to persons specifically briefed on the LIMDIS control protective measures which apply to this information, and that members may be granted access and briefed on these measures only by the designated security manager.

3. I agree that I will advise the security manager when I am reassigned from my present position or otherwise no longer need access to LIMIT (*****) information to provide for removal of my name from the LIMDIS control disclosure list.

24 MAY 1991

SAMPLE LIMITED DISSEMINATION BRIEFING ACKNOWLEDGEMENT

PRIVACY ACT NOTICE: The Privacy Act, 5 USC 552a, requires that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to certify that you have been briefed on the security protective measures which apply to the information identified and defined above. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of your access and possibly result in the denial of your being granted access.

=====

CERTIFICATION:

(*)Signature of Briefing
Official:

(**)Signature of Member
Briefed:

(TYPED NAME OF BRIEFER)

Date: _____

(TYPED NAME OF MEMBER)

Date: _____

=====

24 MAY 1991

CHAPTER 10

TRANSMISSION OF CLASSIFIED MATERIAL

1001. BASIC POLICY

1. Classified information will be transmitted either in the custody of an appropriately cleared individual or by an approved system or carrier, and per the provisions of this Chapter and Chapter 15 of reference (a).

2. The term transmission refers to any movement of classified information or material from one place to another. Unless a specific kind of transportation is restricted, the means of transportation - car, bus, train, ship, plane - is not particularly significant.

3. The carrying of classified material across national borders is not permitted unless arrangements have been made that will preclude customs, postal, or other inspections. In addition, foreign carriers may not be used unless the U.S. escort has physical control of the classified material. (Refer to Chapter 6 for information pertaining to handcarrying classified material.)

1002. TOP SECRET

Top Secret information will be transmitted only by:

1. The Defense Courier Service (DCS). (Refer to paragraph 1013 for further instructions regarding the use of DCS.)

2. The Department of State Courier System.

3. Cleared and designated U.S. military personnel or Government civilian employees traveling on a conveyance owned, controlled or chartered by the Government or a DOD contractor.

4. Cleared and designated U.S. military personnel or Government civilian employees by surface transportation. (See Chapter 6.)

5. Cleared and designated U.S. military personnel or Government civilian employees on scheduled commercial passenger aircraft within and between the U.S., its Territories and Canada, when approved per Chapter 6.

24 MAY 1991

6. Cleared and designated U.S. military personnel and Government civilian employees on scheduled commercial passenger aircraft on flights outside the U.S., its Territories and Canada, when approved per Chapter 6.

7. A cryptographic system authorized by the Director, National Security Agency (NSA).

8. A protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EMSEC) Issuance System. The Protected Wireline Distribution System over which Top Secret information may be transmitted in unencrypted form will be considered for approval by Commander, Naval Security Group Command provided all of the following conditions have been met:

a. All terminal equipment and connecting wirelines are installed per the appropriate RED/BLACK engineering and installation criteria.

b. All end terminal equipment or subscriber sets are located in areas staffed only by personnel cleared for access to Top Secret information. All other personnel are excluded from the areas, except on official business, and then only under continuous surveillance or escort of Top Secret cleared personnel.

c. Every effort is made to install connecting wirelines entirely within areas staffed only by Top Secret cleared personnel and where access is limited as described in subparagraph b above. When this is not possible, those portions of the wireline which must be installed outside of Top Secret control areas must be under direct, continuing and complete control in order to preclude covert interception.

NOTE: The transmittal of Top Secret via U.S. Mail is prohibited.

1003. SECRET

Secret information will be transmitted by:

1. Any of the means approved for the transmission of Top Secret except that Secret material may be introduced into the DCS only when U.S. control of the material cannot otherwise be maintained. This restriction on use of DCS does not apply to sensitive compartmented information (SCI) and COMSEC material. When the Department of State Courier System is to be used for

24 MAY 1991

transmission of Secret material, the Secret material shall be sent by Registered Mail to the State Department Pouch Room. The correct addressing of the inner and outer envelopes for overseas activities is found in the Standard Navy Distribution List (SNDL). As the SNDL lists the addresses for unclassified and classified mail, ensure that the correct address, especially for military attaches is used.

2. U.S. Postal Service Registered Mail within and between the U.S. and its Territories.

3. U.S. Postal Service Registered Mail through Army, Navy, or Air Force Postal Service facilities, outside the area described in paragraph 2 above, provided the mail does not pass through a foreign postal system or any foreign inspection, or via foreign airlines. The material must remain under U.S. control. Special care shall be exercised when sending classified material to U.S. activities overseas. If the material is introduced into a foreign postal system, it has been subjected to compromise. All mail to FPO/APO addresses outside the U.S. and its Territories must be sent via Registered Mail.

4. U.S. Postal Service and Canadian Registered Mail with Registered Mail receipt between U.S. Government and/or Canadian Government installations in the U.S. and Canada.

5. As authorized by DSPP, ODUSD(P) memo of 10 May 89 (NOTAL) and implemented by CNO Memorandum 2220, Ser 09N2/9U651968 of 27 July 89; U.S. Postal Service Express Mail (USPS) for transmission between U.S. Government activities and between U.S. Government activities and contractors, within and between the U.S. and its Territories. USPS Express Mail will not be used for transmission to an APO/FPO address.

a. The use of USPS Express Mail is permitted when it is the most cost effective method of transmittal, given the constraints of time, security and accountability. Because of the cost, use of the USPS Express Mail is strictly controlled within the DON and must be approved in advance by the Head, Correspondence Control, Mail and Files Branch (OP-09B34) for OPNAV, and the Director, Secretariat Support Division for SECNAV. The use of Federal Express for transmittal of classified information is prohibited.

b. The USPS Express Mail envelope will not serve as the outer wrapper. Classified material transmitted by USPS Express Mail will be prepared per paragraph 1011 of this instruction.

24 MAY 1991

c. Under no circumstances will the USPS Express Mail form 11-B, waiver of signature and indemnity be executed even for Confidential material.

d. Until this policy is implemented into reference (a) formally, to avoid misunderstandings, a notice will be attached to the transmitted material (not the envelope) stating that the use of USPS Express Mail is authorized per CNO memorandum 2220, Ser 09N2/9U651968 of 27 July 1989.

6. Carriers as authorized in Chapter 15, paragraphs 15-3.6 and 15-3.7 of reference (a).

7. Electrical means over approved communication circuits to which safeguards have been applied to protect unencrypted classified information in accordance with Chapter 15, paragraph 15-3.8 of reference (a).

1004. CONFIDENTIAL

Confidential information will be transmitted by:

1. Any means approved for the transmission of Secret material; however, use of the U.S. Postal Service for Confidential material is governed by the following:

a. U.S. Postal Service Registered Mail will be used:

(1) For NATO Confidential.

(2) To and from FPO and APO addresses located outside the U.S. and its Territories.

(3) To other addresses when the originator is uncertain that their location is within the U.S.

b. U.S. Postal Service First Class Mail will be used between Department of Defense activities anywhere in the U.S. and its Territories.

c. U.S. Postal Service Certified mail or, if required by subparagraphs a(1) through (3) above, Registered Mail will be used to DOD contractors or to non-DOD agencies of the Executive Branch. First Class Mail is not authorized.

d. USPS Express Mail may be used between DOD activities and DOD contractors within the U.S. and its Territories. However,

24 MAY 1991

because of the cost, use of the USPS Express Mail is strictly controlled within the DON and must be approved in advance by the Head, Correspondence Control, Mail and Files Branch (OP-09B34) for OPNAV, and the Director, Secretariat Support Division for SECNAV.

e. Certified or Registered Mail must be used when sending Confidential mail to the State Department for forwarding by diplomatic pouch. If Certified Mail is not available, Registered Mail will be used.

2. Commercial carriers as outlined in Chapter 15, paragraph 15-4.2 of reference (a).

3. In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens as outlined in Chapter 15, paragraph 15-4.3 of reference (a).

1005. TELEPHONE TRANSMISSION

1. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits.

2. Some offices require staff members to answer telephones with the statement, "This is not a secure line." This practice is not a DON or command security requirement. Approved secure communication systems require equipment and operating procedures to place and receive calls that are quite different from those used for general telephone service. Unless the special equipment is being used, there is no reason to believe a line could be secure. Although the warning may be given as a method of stressing telephone security, all personnel will be instructed that the caller and person being called will know when they are using a secure line. In all other circumstances, with or without the warning, the telephone system is not secure and any discussion of classified information or "talking around" classified information is prohibited.

3. Classified information will not be transmitted over commercially available Data Encryption Standard (DES) Modules in voice land-mobile communications equipment. Such equipment is not approved for the encryption of classified information. Although approved by the National Security Agency (NSA) for encryption of classified information, the new commercially available secure voice module (Motorola "Fascinator") is not

24 MAY 1991

authorized for use by Navy commands for transmission of classified information.

1006. RECEIPT SYSTEM

1. Transmit Top Secret material under a continuous chain of receipts.

2. Cover Secret material by a receipt between directorates, commands and other authorized addresses. Failure to sign and return a receipt to the sender may result in a report of possible compromise or a command security violation report.

3. Receipts for confidential material are not required except when the material is transmitted to a foreign government (including embassies in the U.S.).

4. The sender of the material will attach the receipt to the inner cover. A postcard receipt form, such as OPNAV Form 5511/10 (Record of Receipt), may be used for this purpose. A sample receipt is Exhibit 15A of reference (a). Receipt forms will be unclassified and contain only the information necessary to identify the material being transmitted. Receipts will be retained for at least 2 years. (For OPNAV staff personnel, the receipt form is normally initiated by OP-09B34 when they process and wrap outgoing Secret material.)

5. In those instances where a fly-leaf (page check) form, to be returned to the sender, is used with classified publications, an additional receipt is not necessary.

1007. TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS

The transmission of classified material to foreign governments must meet the requirements of Chapter 15, paragraph 15-7 of reference (a).

1008. TRANSMISSION OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL

Transmit communications security (COMSEC) material per CSP 1, (NOTAL).

1009. TRANSMISSION OF RESTRICTED DATA

Transmit Restricted Data documents in the same manner as other material of the same security classification.

24 MAY 1991

1010. CONSIGNOR-CONSIGNEE RESPONSIBILITY FOR SHIPMENT OF BULKY MATERIAL

Refer to Chapter 15, paragraph 15-10 of reference (a) for procedures regarding consignor-consignee responsibility for shipment of bulky material.

1011. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION

1. Classified material will be properly prepared for transmission to protect it from unauthorized disclosure as outlined in paragraph 15-11 of reference (a).

1012. ADDRESSING

1. Classified material shall be addressed to an official Government activity or DOD contractor and not to an individual. This requirement is not intended to prevent the use of office code numbers or phrases in the address such as "Attention: Mr. John Smith," or similar aids in expediting internal routing, in addition to the organization address. In these cases, an "Attention" line may only appear on the inner envelope or transmittal document.

2. Consult the following for complete and correct mailing addresses and mailing instructions:

a. Current issue of the Standard Navy Distribution List, Part 1, containing the official list of fleet and mobile units and their administrative addresses.

b. Current issue of the Catalog of Naval Shore Activities, including Standard Navy Distribution List, Part 2, containing the official list of shore activities with complete administrative addresses.

c. The Defense Investigative Service, Personnel Investigations Center - Central Verifications Activity (DIS PIC-CVA) is the central activity for verification of DOD contractor facilities facility clearance, safeguarding capability and correct classified mailing address. The DIS PIC-CVA can be reached as follows:

Defense Investigative Service
PIC-CVA
P.O. Box 1211
Baltimore, MD 21203-1211

24 MAY 1991

The PIC-CVA will advise the releasing office in writing, normally within five working days, that the DOD contractor is or is not physically equipped to safeguard the classified material, or state that an evaluation cannot be given and outline the reasons. In this connection, the releasing office shall furnish to the DIS PIC-CVA information available (description, quantity, end item, and classification of the information related to the contract and other facts) to assist them in determining whether the contractor meets the safeguarding requirements of references (a) and (b). Service by the PIC-CVA can be improved by providing them with the Federal Supply or CAGE code of the DOD contractor facility.

In exceptional cases, verification may be furnished by telephone provided the verification is confirmed in writing. The DIS PIC-CVA may be reached from 0800-1700 on commercial telephone number: (301) 633-4820.

Each written verification furnished by the DIS PIC-CVA remains valid for a period of one calendar year from the date of issuance unless otherwise notified (superseded) in writing.

3. The inner envelope or container will show the address of the receiving activity.

4. An outer envelope or container will show the complete and correct address of the recipient and the return address of the sender.

5. Care must be taken to ensure that classified material intended only for the U.S. elements of international staffs or other organizations is addressed specifically to those elements and that the correct address for classified mail is used for overseas locations.

6. When transmitting classified material through the Department of State mail facility for forwarding by diplomatic pouch through the Department of State Courier System, the outer envelope will be addressed to Chief, Classified Pouch and Mail Branch, U.S. Department of State, Washington, D.C. 20520-0528. The inner envelope will be marked with the appropriate classification and addressed to the specific overseas activity.

1013. DEFENSE COURIER SERVICE (DCS)

1. Incoming: All DCS material, including deadline delivery date material, will be picked up by the OPNAV, SECNAV, and JAG Top Secret Control Sections (OPNAV, OP-09B31C2, Room 4C479,

24 MAY 1991

x71156; SECNAV Administration Division, Room 4D680, x51649; and JAG-Code 11). DCS material is picked up from the Pentagon Sub-station, Room 1C240, 0930-1230 Monday through Friday. Only Top Secret Control Section personnel who are listed on a qualified DCS Form 10 may pickup or deliver DCS material with the Pentagon Sub-station or the Washington DCS Station, Fort George G. Meade, MD. The Top Secret Control Sections will control and distribute DCS material as required.

2. Outgoing: The OPNAV, SECNAV and JAG Top Secret Control Sections are responsible for entering material into the DCS system per the DCS Joint Army, Navy and Air Force Regulation, AR 66-5 OPNAVINST 5130.2A AFR 183-2 of 1 October 1982, and subsequent revisions.

24 MAY 1981

CHAPTER 11

SAFEGUARDING AND SECURITY STORAGE

1101. RESPONSIBILITY FOR SAFEGUARDING

1. Anyone who has possession of classified material is responsible for safeguarding it at all times and particularly for locking classified material in appropriate security equipment whenever it is not in use or under direct observation of authorized persons. The custodian must follow procedures which ensure that unauthorized persons do not gain access to classified information by sight or sound or other means. Classified information will not be discussed with or in the presence of unauthorized persons.

2. Personnel will not remove classified material from designated office or working areas except in performance of their official duties and under conditions providing the protection required by this instruction. (See also Chapter 6 on handcarrying in a travel status.) Under no circumstances will personnel remove classified material from designated areas to work on it during off duty hours, or for any other purpose involving personal convenience, without specific approval of the ACNO, DCNO, DSO, ASN or Director of DON Staff Office as applicable. Approval will be given only when there is an overriding need, the required physical safeguards, including a GSA-approved storage container are provided, and a list of the material removed is kept at the command. Approval to remove classified material will not include permission for overnight storage in any location other than a secure government or cleared industrial facility.

1102. SECURITY CONTAINERS

1. General

a. Classified material shall be protected by storage in containers authorized in Chapter 14 of reference (a). The custodians' name shall be indicated on a Standard Form (SF) 700, (Exhibit 11A), and posted on the inside of the container door or combination lock drawer. The custodian shall bear primary responsibility for compliance with security procedures relating to the container and its contents.

b. No security container with wheels affixed is approved for storage of classified material.

24 MAY 1991

2. Control

a. When new storage equipment is received, it will pass through the Security Operations/Personnel Security Section (OP-09B31D) for inspection and numbering.

b. To ensure a complete and accurate control inventory is maintained, no container will be moved from its assigned space without prior written approval of the Head, Security Operations/Personnel Security Section (OP-09B31D).

c. Requests for additional security containers will be submitted as follows:

(1) Office requesting security container prepare an OPNAV Office Service Request (OSR) (OPNAV 5900/3). A written verification on each request will show a current physical security survey has been made of on-hand security equipment and classified records and it has been determined, based upon the survey, that it is not feasible to use available equipment or to retire, return, declassify or destroy a sufficient volume of records currently on hand to make the needed security storage space available. The OSR shall include room number and type of container desired, as well as the justification described above.

(2) Route the OSR to OP-09B32 via OP-09B31.

(3) When the security container is delivered, the custodian must request a new combination change by calling the OPNAV Security Operations Center.

(4) After the combination is changed, the custodian will submit a new SF700 before close of business on the same day the combination is changed. If the work was completed by a contractor the receipt ticket must be returned with the SF700.

d. Excess security containers shall be reported promptly to the Security Operations/Personnel Security Section (OP-09B31D). They must be returned as follows:

(1) Submit an OSR to OP-09B32 via OP-09B31. Ensure security container number is on the request.

(2) Remove all classified material.

(3) OP-09B31 will change or request a contractor to change the combination to factory (50-25-50). If a contractor

24 MAY 1991

changes the combination, the custodian must immediately deliver the contractor invoice to OP-09B31.

(4) OP-09B31 will respond to thoroughly inspect the security container. Upon completion of the inspection OP-09B31 will annotate the OSR that inspection is complete and forward the OSR to OP-09B32.

(5) OP-09B32 will pick up the security container, return it to inventory and notify OP-09B31 when complete.

(6) No security container will be placed in hallways without prior written approval of the Security Operations/Personnel Security Section (OP-09B31D).

e. The Security Operations/Personnel Security Section (OP-09B31D) shall be notified immediately should any doubt arise concerning the state of repair or suitability of any security storage equipment or area. If a problem arises and is not immediately reported, the possibility of a lockout or improperly secured container may exist.

1103. COMBINATIONS

1. Combinations will be changed when containers/locks are first placed in use, at least annually thereafter (unless required more frequently by the type of material stored there), and when any of the following occurs:

a. An individual knowing the combination no longer requires access.

b. The combination has been subject to possible compromise or the security container has been discovered unlocked or unattended.

c. The container (with built-in lock) or the padlock is taken out of service. Built-in combination locks will be reset to the standard combination: 50-25-50. Combination padlocks will be reset to standard combination: 10-20-30.

2. Combination change work shall be performed by the OPNAV Security Force or other qualified personnel designated in writing by the OPNAV Security Manager. To change a safe combination, the requesting office will:

24 MAY 1991

a. Contact OPNAV Security Operations Center to arrange for combination change.

b. After the combination is changed, the requesting office will submit a new SF 700 before the close of business on the same day the combination is changed. Copy 1 of the SF 700 will be affixed to the inside of the container on the combination lock drawer.

c. If a contracted locksmith performs the combination change, the customer receipt ticket must be returned to OPNAV Security on the same day the work is performed.

3. In selecting combination numbers, sequential numbers (i.e., multiples of 5, simple ascending or descending arithmetical series), and personnel data, such as birth dates and Social Security Account numbers will not be used. The same combination will not be used for more than one container in any one classified material control center or secondary control point. In setting a combination, numbers should be used that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

4. To prevent a lockout, two different people should try a new combination before closing the container or vault door.

5. The combination of a secured area or container used for the storage of classified material will be assigned a security classification equal to the highest category of the classified material authorized to be stored in it.

1104. LOCKING PROCEDURES

1. The use of proper locking procedures when securing storage containers is vital to the protection of classified material. Security storage containers should be locked without haste, and must be re-checked by a second person. Use the following procedures:

a. Vaults/MAP and File Safes. Firmly shut door or doors and rotate the combination dial at least four complete revolutions in one direction. Check and re-check.

b. Security Filing Cabinets. These units are manufactured by several firms, and many models are in use. The mechanical arrangements of these cabinets differ between brands and

24 MAY 1991

models. Procedures to secure all of the various models of safe files are:

(1) Shut all drawers other than the combination drawer. Push each drawer in firmly as far as it will go.

(2) Shut combination drawer. Push in firmly as hard as it will go.

(3) If lock has a manipulation proof (MP) knob in dial center, turn MP knob in a counter-clockwise direction to free dial for locking.

(4) Rotate dial at least four complete revolutions in the same direction.

(5) Test each drawer for security by pulling vigorously several times.

(6) CAUTION: If cabinet is re-opened (such as for storage of a last minute paper), ALL of the foregoing must be repeated.

c. Lock-bar Filing Cabinets. Further modification of filing cabinets to bar and padlock type stowage equipment for classified material is prohibited by reference (a). Lock-bar cabinets currently in use need not be replaced until no longer serviceable; however, they shall not be used for storage of material of a higher classification than Secret. They shall be used only with a General Services Administration (GSA) approved manipulation-proof keychange combination padlock bearing a CNOP or SNP number; e.g., P1829. This type of padlock should be checked after locking to ensure that the keyway guard slide (on the back side of the padlock) is in closed (down) position. During working hours, in order to prevent possible substitution of padlocks by unauthorized personnel, open padlocks will not be left on top of the lock-bar cabinets, but will be stowed in the cabinet or locked through the staple until the cabinet is secured at the end of the working day. When securing lock-bar cabinets, care will be taken to see that the bar is properly inserted through all keepers. The combination dial must be rotated at least four complete revolutions in the same direction. Procedures must be employed by custodians of lock-bar filing cabinets to preclude the possibility of papers stowed in these containers from protruding out of the drawers when the cabinets are properly secured. Methods employed may include, but are not limited to:

24 MAY 1991

(1) The insertion of a bound book in the front end of the drawer to prevent individual papers from being removed.

(2) The insertion of stiff cardboard, such as file folders, in the forward portion of the drawer, with one flap in the horizontal position above other papers filed in the drawers, and the other flap in a vertical position at the front of the drawer.

d. Doors with Multiple Locking Devices: Check to ensure combination deadbolt has "caught" by disengaging other locks (cipher, keylock, etc.) and attempting to push the door open.

2. Responsibility for Securing. Direct responsibility is assigned to the designated custodian of each container. In the designated custodian's absence, an alternate custodian shall be designated and specifically charged with the responsibility for proper securing of the container.

1105. OPNAV LOCKSMITH SERVICES

The Head, Security Operations/Personnel Security Section is responsible for all lock work involving room doors, combination locks on doors and security containers assigned within the Pentagon only. For offices located outside the Pentagon, the Head, Security Operations Section is responsible only for the maintenance of security containers. Personnel requesting lock service for office doors outside the Pentagon will contact the appropriate Building Manager's Office. The Head, Security Operations/Personnel Security Section will provide keys for personnel within the Pentagon with the approval of the Security Coordinator. Lost, stolen, damaged or misplaced keys should be promptly reported to the Head, Security Operations Section.

1106. AREAS PROTECTED BY ELECTRONIC ALARM SYSTEMS

1. Electronic alarm systems may be installed in critical areas as a means of supplementing security storage equipment, but such protection is not intended to replace such equipment. Intrusion detection systems are designed to detect, not prevent, an attempted intrusion. Because of their cost, alarm systems are justified only when their use will result in a commensurate reduction or replacement of other protective elements without loss of protection effectiveness. Classified information located within alarmed areas shall be protected by the highest standard of security containers possible without detriment to the mission of the office concerned. Any deviation from this standard must

24 MAY 1991

be approved in writing by the Head, Security Operations/Personnel Security Section.

2. Open storage of classified material must be limited to material up to and including SECRET in areas accredited for SECRET open storage. Open storage of TOP SECRET material is permitted only areas presently accredited for TOP SECRET open storage. Open storage accreditation does not apply to any special access program material such as NATO, SIOP or CNWDI. An alarmed area approved for open storage shall be designated as a vault-type room and must conform to the following standards:

a. Access door be secured with a built-in Group 1-R three position, dial type, changeable combination lock. One access door will be permitted in each alarmed area. This door shall be equipped with an automatic door closer and shall not be left open unless continuously manned and under direct observation of cleared personnel.

b. All doors other than the access door must be secured with a positive lock from inside the area to prevent access by use of a key from the outside.

c. All doors will be solid (no vents or windows).

d. All false overheads must be alarmed.

e. Windows and doors must be alarmed. Windows shall be permanently closed. Those doors not solidly constructed must have proximity grid alarms to detect forced entry as well as door switch alarms to indicate opening.

3. As an intrusion detection system's coverage of an area is fixed on installation, it may be greatly affected by changes in the area's physical structure. For this reason changes will be kept to a minimum. An impact assessment and possible reconfiguration of the alarm system may be necessary if alterations, construction or modifications are performed to an office layout. The Head, Security Operations/Personnel Security Section must be notified at least two (2) months prior to commencement of construction, modification, or alterations of an alarmed area.

4. When vacating an alarmed area, the custodian shall ensure the area is free of classified material and formally relinquish custody of the space by contacting the Head, Security Operations/Personnel Security Section. While inspecting the area, particular attention should be paid to desks, filing cabinets, etc. left

24 MAY 1991

behind. On request of the custodian and contingent on availability of security personnel, OPNAV Security will assist the custodian in sweeping the area for classified material. The custodian will turn over all keys and combinations to the Head, Security Operations/Personnel Security Section.

1107. OPENING AND SECURING ALARM AREAS

1. Access Lists. Personnel authorized to open or secure alarmed areas shall be listed on the area's Alarmed Area Access List (OPNAV 5512/6 (Rev. 5-89), Exhibit 11B). All lists for newly alarmed areas, or upon modification to an alarmed area onto the Intrusion Detection Access Control (IDAC) System will be submitted to the Head, Security Operations/Personnel Security Section. Lists will be submitted to the OPNAV Security Operations Center under the following circumstances:

a. Whenever an individual knowing the combination to the area or an individual assigned a Personnel Identification Number (PIN), no longer requires access,

b. Any name changes (marriage, etc.) or phone changes (home or office),

c. When the combination has been compromised, an individual's PIN has been compromised, or the area has been discovered unlocked and unattended, or

d. At least annually, unless more frequent change is dictated by the type of material stored therein. One addition or deletion per page to each access list will be permitted by designated custodian or alternate custodian. The addition or deletion must be submitted by a signed memoranda or by the custodian, alternate custodian in person. All deletions to an access list will be attached, listing last name, first name, middle initial, social security number, and if applicable, card number. Lists should be typed, last name first in alphabetical order with the names of the custodian and alternate custodian appearing first. Failure to maintain a current access list could result in denied access.

2. Securing Requirements. When the alarmed area is unmanned between the hours of 1800-0700 weekdays and at all times weekends and holidays, secure the combination lock and set alarm system in "secure". Between the hours of 0700-1800 Monday - Friday, when alarmed areas must be unattended for 30 minutes or

24 MAY 1991

less, the combination lock must be secured and all non-primary entrance doors bolted shut.

3. Opening Procedures for Alarmed Areas on the (IDAC) System. Personnel entering the alarmed area shall immediately enter their Personal Identification Number (PIN) and enter ACCESS on the Access Control Unit (ACU) keypad.

4. Securing Procedures for Alarmed Areas on (IDAC) System

a. Personnel securing alarmed areas shall ensure the ALARM system indicator light on the ACU is green. Enter "PIN" and enter "SECURE" on the ACU keypad. Exit space, close door, await tone from ACU to indicate that the area is properly secured. If the area is properly secured, a LONG STEADY HIGH PITCHED TONE will sound. If the area is not properly secured, an INTERMITTENT HIGH PITCHED TONE will sound (approximately 4 to 5 pulses.) After the long steady high pitched tone is heard, secure the combination lock.

b. Should difficulty be experienced when placing alarm system in access or secure, contact the OPNAV Security Operations Center at x53667 and state name, CARD number and area number being accessed or secured.

1108. UNALARMED WORK SPACES

1. After normal working hours, unalarmed spaces will be locked with a deadbolt lock. Electrically actuated locks do not afford the degree of protection required for equipment. These locks may be used during normal duty hours for access control only.

1109. CARE OF WORKING SPACES

1. During working hours use the following precautions to prevent access to classified information by unauthorized persons.

a. Monitor the entrance to office spaces and do not give uncleared personnel freedom of movement within the office space. Escort visitors and question unescorted strangers found within the space.

b. When classified documents are removed from storage for working purposes, they will be kept under constant surveillance and face down or covered when not in use. Cover sheets

24 MAY 1981

Standard Forms 703, 704 and 705 for, respectively, Top Secret, Secret and Confidential documents shall be used for this purpose.

c. Classified information will be discussed only when unauthorized persons cannot overhear the discussion. Particular care should be taken when there are visitors or workmen in the area.

d. Preliminary drafts, carbon sheets, typewriter and printer ribbons, plates, stencils, stenographic notes, work-sheets, and all similar items containing classified information will be protected either by destroying them by a method approved for destroying classified material immediately after they have served their purposes, or by giving them the same classification and safeguarding them in the same manner as the classified material they provided.

e. Two-Person Integrity Requirement. Personnel will not normally be permitted to work alone in areas where Top Secret information or information controlled under Special Access Program procedures is used or stored and is accessible to those employees. This policy, however, does not apply in those situations where one employee with access is left alone for brief periods during normal duty hours. It does not require that both employees have equal access, or that a "no lone zone" be established around Top Secret, nor is the requirement as stringent as the two-person control requirement for Communications Security Material Systems (CMS). The two-person integrity requirement must be strictly adhered to outside of normal duty hours. When compelling operational requirements indicate the need, this requirement may be waived in specific limited instances not cited above by CNO (OP-09N). If compelling operational requirements would not enable meeting this requirement, Security Coordinators must submit the specific case(s) with all pertinent information to OP-09B31 for review and coordination with CNO (OP-09N) to determine if a request for waiver is required. DO NOT SUBMIT WAIVER REQUESTS DIRECTLY TO CNO (OP-09N).

2. Tops of security containers should be cleared of extraneous material, distinctive cover sheets should be used and classified material should never be placed in desks. These measures will help prevent classified material from being intermingled with unclassified and overlooked when securing. If possible, all desks should be cleared when securing each day (clean desk policy.)

24 MAY 1991

1110. SECURITY CHECK LISTS

1. An Activity Security Checklist (Standard Form 701) shall be used and conspicuously posted in each room near the exit. Security Container Check Sheet (Standard Form 702) shall be posted on all security containers.

2. A division double-check procedure using a second person, shall be employed wherever possible. Persons working late shall be listed as exceptions and are responsible for ensuring the security of their work area prior to departure.

3. After 1800 on weekdays and 1600 on weekends the OPNAV Security Watch (x53667 or x53121) shall assist personnel securing their individual work areas, on an as available basis. Individuals requesting double-checks must REMAIN IN THE AREA until the double-check is completed. OPNAV Security Watch personnel shall not be utilized to perform divisional doublecheck responsibilities.

4. Retain security check lists for a minimum of two years.

5. Sample procedures for security checks can be found in Exhibit 11C.

1111. KEY AND LOCK CONTROL

1. General. Primary responsibility for key control rests with the Head, Security Operations/Personnel Security Section (OP-09B31D), who will act as the Key Control Officer. Each ACNO, DCNO, DSO, Assistant Secretary of the Navy and Director of Department of the Navy Staff Office Security Coordinator will act as Key Custodian for his/her organization and will be responsible to the Key Control Officer for key control matters.

2. Responsibilities

a. The Key Control Officer (OP-09B31D) is responsible to the OPNAV Security Manager for all security related key and lock control functions and will conduct an annual inventory of all keys and padlocks issued.

b. Security Coordinators shall conduct a semi-annual inventory of all keys issued to his/her custodial or subcustodial accounts and assist the Key Control Officer in his/her annual survey. During an inventory, the Security Coordinator will personally sight all assigned keys. Security Coordinators shall

24 MAY 1991

forward inventory results together with any discrepancies to the Key Control Officer. When unauthorized duplication or lost keys are discovered, the Security Coordinator will immediately inform the Key Control Officer. When office doors are replaced or removed, Security Coordinators must ensure that original locks are either reinstalled or turned in to the Key Control Officer. To facilitate recovery of keys when employees leave, Security Coordinators should ask supervisors to inform them when key-holders give notice or receive permanent change of station (PCS) orders. Security Coordinators must also provide the OPNAV Security Operations Center, Room 4A654, with a list of personnel authorized to check out a room key. It should be remembered that such personnel will have unlimited access to the office at all hours. Update lists whenever personnel changes occur.

c. The individual to whom a key is issued is responsible both for the key's whereabouts and for returning it to their Security Coordinator on request, when transferring, separating, etc. Any transfer of custody will be made through the Security Coordinator. Personnel will not loan their key to anyone or turn it over to their relief directly. Individuals must produce their keys at least twice yearly to be inventoried. Personnel must report lost or defective keys and locks to their Security Coordinator. In the Security Coordinator's absence, contact the Key Control Officer in Room 4A654, x53667. Do not mark keys with information (name, room, office code) that might help unauthorized personnel use a lost key.

3. Key Control Records/Logs. Records maintained by Security Coordinators must show the number of keys on hand for each room, number issued, to whom, date/time of issue or return, and the signature of personnel checking out or returning security keys. Continuous accountability is required.

4. Issuance of Keys. Issuance will be determined by need. Convenience, rank or status is not sufficient criteria for issuance of a security key. The OPNAV Security Manager is responsible for developing and enforcing rules governing key issuance and must approve any changes or exceptions to existing policy.

a. Determination of which personnel within an office will receive keys should be made by the office's senior person.

b. Only five keys will be provided to any one office or office suite.

24 MAY 1991

c. The OPNAV Security Operations Center will maintain one additional key for each office in Room 4A654. This key will be available 24 hours a day for temporary issuance to personnel listed on the room's access list who present proper identification. The key must be returned by close of business each day. Habitual failure to return the key may result in revocation of the check-out privilege. Names on access lists should be typed, last name first, in alphabetical order. Names of personnel on the access list who are issued a permanent key should be marked with an asterisk (*).

d. Naval Reserve members should arrange for access to offices by coordination with their host office/activity. A Security Coordinator may place Reservists' names on a room's access list permanently or as the need for access arises.

5. Duplication of Keys. Security keys will not be duplicated except through the Key Control Officer. Unauthorized duplication could result in administrative actions.

6. Alarmed Areas. Doors to alarmed areas will not be equipped with keylocks. Alarmed area main access doors only require a #50 S & G built-in Group 1-R three position, dial type, changeable combination lock. All non-primary entrance doors must be equipped with a 181 sliding dead-bolt on the inside of the door. These doors shall be used for emergency exit only. If a non-primary door must be opened temporarily (i.e., move furniture, carpet replacement, etc.), notify OPNAV Security of the situation.

24 MAY 1991

EXHIBIT 11A

SECURITY CONTAINER INFORMATION
(STANDARD FORM 700)

TOP SECRET		TOP SECRET				
SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP) 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER 3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER 4. DETACH PART 2A AND INSERT IN ENVELOPE 5. SEE PRIVACY ACT STATEMENT ON REVERSE				1. AREA OR POST (if required) N/A	2. BUILDING (if required) PENTAGON	3. ROOM NO 6A999
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE) OP-0X				5. CONTAINER NO CNOF-XXXX		
6. MFG & TYPE CONTAINER N/A		7. MFG & TYPE LOCK N/A		8. DATE COMBINATION 89MAR01		
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE JOHN DOE/						
10. Immediately notify one of the following persons, if the container is found open and unattended						
EMPLOYEE NAME		HOME ADDRESS		HOME PHONE		
DOE, JOHN NMN		N/A		(703) XXX-XXXX		
AND NO OTHERS						

1. ATTACH TO INSIDE OF CONTAINER

700-103
NSN 7540-01-214-3372

STANDARD FORM 700 (8-85)
Prescribed by GSA/1500
32 CFR 2003

U.S. GOVERNMENT PRINTING OFFICE: 1987 - 175-285

WARNING
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE OPENED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

CONTAINER NUMBER
CNOF-XXXX

COMBINATION

DETACH HERE

3 turns to the (Right) (Left) stop at 3

2 turns to the (Right) (Left) stop at 20

1 turns to the (Right) (Left) stop at 30

0 turns to the (Right) (Left) stop at 77

WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UNLESS INDICATED OTHERWISE

TOP SECRET

2A INSERT IN ENVELOPE

32 CFR 2003

PLACE IN ENVELOPE
AND SEAL

NOTE: TOP SECRET FOR TRAINING; OTHERWISE UNCLASSIFIED

24 MAY 1991

EXHIBIT 11A

SECURITY CONTAINER INFORMATION
(STANDARD FORM 700)

SECURITY CONTAINER INFORMATION		
INSTRUCTIONS		
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP)	2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER	3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER
4. DETACH PART 2A AND INSERT IN ENVELOPE	5. SEE PRIVACY ACT STATEMENT ON REVERSE	
10. Immediately notify one of the following persons if this container is found open and unattended		
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE
DOE, JOHN M.	N/A	(703) XXX-XXXX
CRAMP, JOHN A.	N/A	(703) XXX-XXXX

1. ATTACH TO INSIDE OF CONTAINER

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOC
32 CFR 2003

CONTAINER NUMBER
ZONE 399

COMBINATION

3	turn to the (Right) (Left) stop at	1
2	turn to the (Right) (Left) stop at	2
1	turn to the (Right) (Left) stop at	12
0	turn to the (Right) (Left) stop at	21

DETACH HERE

WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED
UNCLASSIFIED DISCHARGE BY 2001-01-01

2A INSERT IN ENVELOPE

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOC
32 CFR 2003

PLACE IN ENVELOPE
AND SEAL

NOTE: TOP SECRET FOR TRAINING; OTHERWISE UNCLASSIFIED

24 MAY 1991

EXHIBIT 11B

ALARMED AREA ACCESS LIST
(OPNAV FORM 5512-6)

ALARMED AREA ACCESS LIST OPNAV 5512-6 REV (5-89)		AREA NUMBER 399		MONTH, YEAR MARCH, 1999		OFFICE CODE OP-0X	
NAME LAST FIRST MI SSN	RANK RATE GRADE	CARD NUMBER	NAME LAST FIRST MI SSN	RANK RATE GRADE	CARD NUMBER		
CUSTODIAN							
DOE, JOHN NMN 111-45-1111	CAPT	XXX					
ALTERNATE CUSTODIAN							
CRAMP, JOHN A. 216-45-3333	CDR	XXX					
ALCOTT, GEORGE P. 345-34-5345	CDR	XXX					
BARNSTORMER, JAY L. 111-34-1111	CDR	XXX					
COP, ROGER R. 111-11-1111	LT	XXX					
WILLIAMS, DOG R. 111-12-1111	GS-7	XXX					
AND NO OTHERS							
CUSTODIAN'S TYPED NAME AND SIGNATURE DOE, JOHN NMN <i>John Doe</i>						OFFICE PHONE NUMBER X99999	HOME PHONE NUMBER (703) XXX-XXXX
ALTERNATE CUSTODIAN'S TYPED NAME CRAMP, JOHN A. <i>John A Cramp</i>						OFFICE PHONE NUMBER X00000	HOME PHONE NUMBER (301) XXX-XXXX
AREA NUMBER 399	ZONE NUMBER 712-715	ROOM NUMBER 6A999	ACCESS THROUGH 6A999	REMARKS LIST PERSONNEL NAMES ALPHABETICALLY N/A			

24 MAY 1991

EXHIBIT 11C

**SAMPLE PROCEDURES FOR SECURITY CHECK AT THE END
OF THE WORKING DAY**

1. Each individual must be sure his or her working area is secure at the end of the working day by:

- a. Looking on top of, under, behind and in desks.
- b. Making sure that working trays and baskets are empty.
- c. Properly storing or shredding notes, carbon paper, rough drafts or similar working papers.
- d. Placing classified documents, correspondence or related classified material in proper security containers.
- e. Securely closing each drawer of the security container and locking the container by rotating the dial at least four complete turns in the same direction.
- f. Checking the locking drawer to make sure the container is secured.
- g. Surveying the general area to be sure nothing is unsecured. This includes looking on top of and in between security containers, general storage cabinets, working tables and checking trash cans.

2. Each week, a staff member will be assigned responsibility for double-checking the spaces to ensure that they have been secured, using the daily security checklist. Each item on the list will be checked and initialed. The double-checker will ensure that:

- a. All security containers in the area are closed and locked by rotating the combination dial four times in the same direction and trying the locking drawer.
- b. The disks and printer ribbon are removed from word processors.
- c. The reproduction machine is cleared by running it once and checking the reproduction paper for impressions. Machines will be turned off on weekends and holidays.

24 MAY 1991

d. The shredder is cleared. The shred receptacle will be checked to ensure that the residue is from more than ten shredded pages.

e. The telecopier is cleared.

f. Security container tops are cleared.

g. Individual office spaces are cleared.

h. Desk tops and trays are cleared.

i. Typewriter ribbons are removed from those machines using carbon ribbons, on which classified information has been typed.

j. Any electrical appliances are disconnected.

k. The general area is surveyed.

l. If anyone is still working in the area, with a security container open, he or she is listed as an exception, beside the item on the checklist which has not been secured. That person will then be responsible for securing the item, double checking, and initialing the checklist, showing the time of securing.

3. Each individual is responsible for performing the security responsibilities assigned. It is the individual's responsibility to arrange with the Security Coordinator for a substitute to perform the double-check when absence is anticipated. In the unplanned absence of the assigned doublechecker, the Security Coordinator will designate a substitute.

24 MAY 1991

CHAPTER 12**DESTRUCTION OF CLASSIFIED MATERIAL****1201. GENERAL**

The Director, Washington Headquarters Services, Physical Security Division prescribes policy for the destruction of classified material within the Pentagon. The Director is responsible to supervise the destruction of classified material at the Pentagon Incinerator Facility, develop procedures for use of the facility, and schedules the use of the facility.

1202. PROCEDURES

1. Classified material shall be placed in destruction bags, at the office level, in the presence of two witnessing personnel. Two persons will be responsible for transporting burn bags to the OPNAV Security Office, Room 4A654.

2. All bags delivered to the OPNAV Security Office will be documented on a Classified Material Destruction Manifest (OPNAV 5511/57) as shown in Exhibit 12A. Bags will not be over 1/2 full and will be stapled shut. Bags containing large books and computer printouts will be 1/4 full or double bagged and stapled shut. All bags must be marked with a felt pen to show Division (OP-Code), name of responsible official, phone number, highest level of classified material within the bag, and serialized (except for bags containing TOP SECRET). Any bags not meeting the above specifications will be returned to the cognizant office for rebagging.

1203. DESTRUCTION REPORTS

All personnel will record the destruction of SECRET material. Destruction of TOP SECRET material shall be accomplished by the cognizant directorate TSCO. Destruction may be recorded on the OPNAV Form 5511/12 (Classified Material Destruction) or any other record which includes complete identification of material, number of copies destroyed, and the date of destruction. Two officials will be responsible for destroying TOP SECRET and SECRET material and will sign the record of destruction as witnessing the destruction when the material is placed in the burn bag. Records of destruction will be retained for two years. In cases where the originator states that a document "may be destroyed without report" does not change the requirement to record destruction.

24 MAY 1991

This means that the originator does not need to know the document was destroyed.

1204. MESSAGE TRAFFIC

1. Unclassified message traffic, except Naval Nuclear Propulsion Information (NNPI), does not have to be destroyed as classified material. Offices with high volumes of classified and unclassified message traffic may destroy all messages to ensure efficient handling and to preclude inadvertent disposal of classified material. "For Official Use Only" (FOUO) messages will be destroyed by tearing each copy into pieces to preclude reconstruction, and placing them in regular trash containers as required by SECNAVINST 5720.42D for all FOUO materials.

2. The requirement for recorded destruction of routine short life SECRET message traffic received from the Joint Communication Center has been waived for this command because of the high volume of message traffic. SECRET messages must still be destroyed by authorized means and by authorized persons.

1205. DESTRUCTION OF CMS MATERIAL

COMSEC and other CMS material will be accepted in the COMSEC Material System Vault, Room 4A660 from 0800-1100 each working day. It will be accepted at all other times in Voice Communications Maintenance (VCM), Room 4C663, which is open 24 hours a day.

1206. DECLASSIFYING OR CLEARING ADP MEDIA

Declassifying ADP media is a procedure to erase totally all classified information stored in the media. Clearing ADP media is a procedure to erase classified information that lacks the totality and finality of declassifying. The two procedures are distinguished by the specific techniques used and the purpose for which each is done. Refer to paragraph 17-4 of reference (a) for specific guidance on declassifying or clearing ADP media.

1207. EMERGENCY DESTRUCTION PROCEDURES

Mass destruction or total removal of classified material is not considered feasible within OPNAV/SECNAV/DON Staff Offices.

CLASSIFIED MATERIAL DESTRUCTION MANIFEST
(OPNAV FORM 5511/57)

12A-1

24 MAY 1991

CHAPTER 13

OPNAV SECURITY WATCH

1301. GENERAL

An OPNAV Security Watch is maintained on a 24-hour basis to provide physical security supervision of Department of the Navy spaces in the Pentagon. This watch is operated from the OPNAV Security Operations Center, Room 4A654. Overall responsibility for the OPNAV Security Watch rests with the OPNAV Security Manager (OP-09B31) who shall establish standard operating procedures for the watch. The OPNAV Security Watch Force is supervised by the Head, Security Operations/Personnel Security Section. Only members of the OPNAV Security Force, as trained, qualified and certified by the OPNAV Security Manager will be assigned to the OPNAV Security Watch. The Security Watch is composed of a Senior Watchstander, Patrolmen and Marine Corps sentries.

1302. DUTIES AND RESPONSIBILITIES

The OPNAV Security Force, in the performance of duty shall ensure the physical security integrity of assigned Department of the Navy spaces in the Pentagon. Specific duties include:

1. Immediate response to duress alarm enunciation in the offices of the Chief of Naval Operations or the Secretary of the Navy. On such occurrence, a crisis response team will be dispatched so as to arrive on the scene within two (2) minutes of the alarm. The crisis response team shall take appropriate action at the scene to neutralize the crisis until relieved by the Defense Protective Service (DPS).

2. Monitor the security of specially alarmed zones and dispatch the crisis response team when an unauthorized intrusion occurs and activates the alarm.

3. Conduct daily security inspections of the Department of the Navy spaces in the Pentagon.

4. Assist the DPS as required in the event of natural disaster or bomb threats.

5. Perform such other duties that are assigned by proper authority.

24 MAY 1991

1303. USE OF ARMS

Members of the OPNAV Security Force will be armed while in a duty status. The OPNAV Security Manager is responsible for training, qualifying and certifying members of the OPNAV Security Force in the use of arms prior to their assignment to the OPNAV Security Watch. Certified members shall carry a completed current authorization form (OPNAV 5512/1) at all times. The OPNAV Security Force will also be responsible to comply with firearms policies as set forth in the Standard Operating Procedures guide.

24 MAY 1991

CHAPTER 14**VISITS AND MEETINGS****1401. GENERAL**

1. Basic policy regarding visits and meetings is found in Chapters 18 and 19 of reference (a).
2. For security purposes, the term visitor applies to:
 - a. Any person who is not attached to or employed by the command.
 - b. Personnel on temporary additional duty.
3. Under no circumstances may personnel handcarry their own visit request(s) as proof of clearance.

1402. OUTGOING VISITS

1. Visit Requests (Visitor Clearance Data Forms, OPNAV 5521/27, Exhibit 14A) will be completed as proof of clearance for classified visits by OPNAV, SECNAV and DON Staff Office personnel. Cognizant Security Coordinators or Assistants will verify accuracy of data, sign, and mail visit requests to appropriate host activities. Emergency visit clearances may be passed by telephone, provided that this is acceptable to the host activity. They must be followed-up as soon as possible by hard copies. Requests for visits between Navy commands may be transmitted by facsimile machines and must be on official letterhead or OPNAV 5521/27. Visit requests submitted by facsimile machines must include all of the required information.

2. When access to classified information is required in connection with a visit to a contractor facility, the Security Coordinator or Assistant must submit a visit request directly to the contractor, with an information copy to the appropriate Defense Investigative Service Regional Director of Industrial Security (DIS Cognizant Security Office). A list of these addresses may be found in Appendix C of reference (a).

1403. INCOMING VISITS

1. The OPNAV Security Branch (OP-09B31) is the central point for receiving and reviewing incoming visit requests from all

24 MAY 1991

outside activities. Any office receiving visit requests directly must forward them to the OPNAV Security Branch (OP-09B31).

a. Incoming visit requests from other DOD or government organizations must be submitted per the requirements of reference (a). OP-09B31D will then forward them with a security review endorsement to the cognizant Security Coordinator (or Assistant) for further dissemination or final disposition/retention. Visit requests not prepared per reference (a) will be returned to the submitting DOD or government organization.

b. Incoming visit requests from contractor facilities must be submitted per the requirements of the Industrial Security Manual for Safeguarding Classified Information (ISM) (DOD 5220.22-M) of March 1989 (NOTAL). OP-09B31C will then forward them with a security review endorsement to the cognizant Security Coordinator (or Assistant) for further dissemination or final disposition/retention. Visit requests not prepared per DOD 5220.22-M of March 1989 (NOTAL) will be returned to the contractor facility.

2. Before access to classified information may be granted to a visitor, the host office must:

a. Check visitor identification, i.e. government/contractor picture ID badge or drivers' license.

b. Have on file a valid visit request with the visitor's security clearance endorsed by OP-09B31C or OP-09B31D as applicable.

c. Confirm the visitor's "need-to-know" with the appropriate program/project manager.

NOTE: Refer to Chapter 15 for in-depth information regarding access by contractor personnel.

1404. VISITS TO DEPARTMENT OF ENERGY (DOE) ACTIVITIES

1. Request for Visit or Access Approval (DOE F5631.20), Exhibit 14B, must be completed for visits to DOE activities and related contractors. The initiating office will forward the completed form including a typed addressed envelope to the OPNAV Security Branch (OP-09B31D) days in advance, to allow sufficient time for processing and mailing.

24 MAY 1991

2. The "To" address block will be filled in with the address of the appropriate DOE activity or contractor facility, unless the visit requires access to weapons related Restricted Data or Critical Nuclear Weapons Design Information (CNWDI). In such cases, the requesting office will leave the "To" block and the accompanying envelope blank, to be completed by OP-09B31D.

1405. VISITS BY MEMBERS OF CONGRESS

1. Visits by Members of Congress are normally arranged by the Office of the Chief of Legislative Affairs or Department of the Navy officials who will inform the office to be visited of the general level and disclosure level of classified information.

2. Guidance concerning disclosure of classified information should be obtained as soon as possible from the Office of the Chief of Legislative Affairs.

3. Members of Congress, by virtue of their elected status, do not require DOD security clearances. Certification of clearance is required, however, for staff members accompanying a Member of Congress (See paragraph 23-2 of reference (a)).

1406. VISITS BY REPRESENTATIVES OF THE GENERAL ACCOUNTING OFFICE

Properly cleared and identified representatives of the General Accounting Office (GAO) may be granted access to classified Department of the Navy information in the performance of their assigned duties and responsibilities per paragraph 18-8 of reference (a).

1407. VISITS BY FOREIGN NATIONALS

1. Policy and procedures for visits by foreign nationals are described in detail in OPNAVINST 5510.48J (NOTAL). Policy and procedures for visits of nationals from communist controlled countries are contained in OPNAVINST C5510.159 (NOTAL).

2. Visits by foreign nationals which will involve substantive technical discussions or the disclosure of classified information require the approval of the Navy International Programs Office (Code 10), or an authority specifically delegated in OPNAVINST 5510.48J (NOTAL).

24 MAY 1991

1408. CLASSIFIED MEETINGS

1. Any meeting which will involve the disclosure of classified information must be held at a government installation or cleared DOD contractor facility.

2. See Chapter 19 of reference (a) and OPNAV NOTICE 5510 of 31 October 1989 for detailed responsibilities for security sponsorship of classified meetings, specific security procedures for classified meetings and procedures for obtaining clearance for non-government attendees.

3. Conference Rooms

a. Protection of classified information within a conference room is the responsibility of the official sponsoring the meeting.

b. The official holding a TOP SECRET meeting in a conference room which is not alarmed will notify the OPNAV Security Manager (OP-09B31) at least 30 working days in advance so that a Technical Surveillance Countermeasures Survey (TSCM) can be scheduled and conducted.

(1) Requests for TSCMs, should state specific room number and date of meeting and will be classified Secret. Declassification statement to be placed on your request is:

Classified by OPNAVINST S5513.4C, Encl. (17)
Declassify on OADR

(2) Upon completion of the survey the official sponsoring the conference is responsible for providing access control of the conference area until the conference is over.

c. Meetings classified SECRET or above require a monitor while the conference is in session. Monitors must have a security clearance equivalent to the classification of material to be discussed. They must provide access control by ensuring that personnel attending the conference have clearance equal to or higher than level of information to be discussed and a "need-to-know".

d. Telephones located in conference rooms shall be disconnected during classified discussions.

24 MAY 1991

1409. UNCLASSIFIED MEETINGS

1. Material prepared for presentation at unclassified meetings and instructional courses on subjects concerning sensitive research and operations should be submitted for security review.

2. Guidance as to categories of information requiring review (see exhibit 12A of reference (a)) and the administrative procedures for submitting the information for review are found in SECNAVINST 5720.44A.

24 MAY 1991

EXHIBIT 14A

VISITOR CLEARANCE DATA FORM
(OPNAV FORM 5521/27)

VISIT REQUEST VISITOR CLEARANCE DATA OPNAV 5521/27 (REV. 1-75) S/N 0107 - LF - 055 - 2235 (SEE CURRENT EDITION OF OPNAVINST. 5510.1 FOR DETAILED INSTRUCTIONS)		PRIVACY ACT STATEMENT ON REVERSE CHECK ONE <input type="checkbox"/> REPLY REQUIRED <input checked="" type="checkbox"/> REPLY ONLY IF NEGATIVE																																				
FROM (COMPLETE ADDRESS OF REQUESTING ACTIVITY) (YOUR COMPLETE MAILING ADDRESS)		DATE OF REQUEST (DATE SUBMITTED) SPECIFIC PERSONNEL OR SECTION OF COMMAND TO BE VISITED (YOU MUST FILL IN THE NAME OF YOUR POINT OF CONTACT)																																				
(COMPLETE MAILING ADDRESS OF ACTIVITY TO BE VISITED)		<div style="font-size: 4em; transform: rotate(-15deg); opacity: 0.5;">SAMPLE</div>																																				
FOLD ON THIS LINE																																						
DURATION OF VISIT (ARRIVE) (FIRST DAY OF THE VISIT)	(DEPART) (NOT TO EXCEED 1 YR) (LAST DAY OF VISIT)	DEGREE OF ACCESS REQUIRED SECRET																																				
PURPOSE OF VISIT/REMARKS (IF THE VISIT IS TO A CONTRACTOR FACILITY, INCLUDE CONTRACT NUMBER IF APPROPRIATE) (INDICATE SPECIFIC PURPOSE.) ALSO INCLUDE CONTRACT NUMBER IF VISITING A CONTRACTOR.																																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">NAME, RANK, TITLE OR POSITION, SOCIAL SECURITY NO.</th> <th style="width: 15%;">DATE AND PLACE OF BIRTH</th> <th style="width: 25%;">NATIONALITY (CHECK ONE)</th> <th style="width: 20%;">LEVEL OF SECURITY CLEARANCE</th> </tr> </thead> <tbody> <tr> <td>JOHN T. DOE 001-01-0001 SECURITY SPECIALIST</td> <td>02-26-55 WASH, DC</td> <td><input checked="" type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td rowspan="2">TOP SECRET</td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td><input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN</td> <td> </td> </tr> </tbody> </table>				NAME, RANK, TITLE OR POSITION, SOCIAL SECURITY NO.	DATE AND PLACE OF BIRTH	NATIONALITY (CHECK ONE)	LEVEL OF SECURITY CLEARANCE	JOHN T. DOE 001-01-0001 SECURITY SPECIALIST	02-26-55 WASH, DC	<input checked="" type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN	TOP SECRET			<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN			<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN				<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN				<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN				<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN				<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN				<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN	
NAME, RANK, TITLE OR POSITION, SOCIAL SECURITY NO.	DATE AND PLACE OF BIRTH	NATIONALITY (CHECK ONE)	LEVEL OF SECURITY CLEARANCE																																			
JOHN T. DOE 001-01-0001 SECURITY SPECIALIST	02-26-55 WASH, DC	<input checked="" type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN	TOP SECRET																																			
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
		<input type="checkbox"/> U.S. CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN																																				
NAME, RANK AND TITLE OF OFFICIAL AUTHORIZING VISIT AND CLEARANCE CDR ROBERT C. SMITH SECURITY COORDINATOR (OP-099) COPY TO (AS REQUIRED)		SIGNATURE 																																				

24 MAY 1991

EXHIBIT 14B

REQUEST FOR VISIT OR ACCESS APPROVAL

(DOE F5631.20)

U.S. GPO: 1988-O-215-898/90535

DOE F 5631.20
(2-87)
(Formerly DP-277)

U.S. DEPARTMENT OF ENERGY
REQUEST FOR VISIT OR ACCESS APPROVAL
(Not to be used for temporary or permanent personnel assignments.)

OMB Control
No. 1010-1800

PART "A"

To: **FILL IN** (except when access to RD or
CNWDI is required for visit)
From: **FILL IN**

Date: **FILL IN**
Prepared by: **FILL IN** (TYPIST)
Symbol: **FILL IN** (OFFICE CODE)
Telephone No.-Commercial: **FILL IN**

It is requested that the following person(s) be granted visit/access approval:

LAST NAME, FIRST, MIDDLE INITIAL AND SOCIAL SECURITY NUMBER	CHECK		DATE OF BIRTH	ORGANIZATION	TYPE CLEARANCE	CLEARANCE NO.	DATE OF CLEARANCE
	U.S. CITIZEN	ALIEN					
INCLUDE POSITION TITLE AND INDICATE ALL INFORMATION REQUIRED	FILL IN		FILL IN	FILL IN	FILL IN	LEAVE BLANK	FILL IN

NAME OF FACILITY(IES) TO BE VISITED:
FILL IN

FOR THE INCLUSIVE DATES:
FILL IN (ie)
1/1/89-12/31/89

DOE Security Official Verifying DOE
Clearance

FOR THE PURPOSE OF:

FILL IN
TO COMPLY WITH THE FOLLOWING PERSON(S):
FILL IN

SPECIFIC INFORMATION TO WHICH ACCESS IS REQUESTED:
FILL IN, IF APPLICABLE

Prior arrangements have/have not been made as follows:
FILL IN, IF APPLICABLE

MARK BLOCKS
Access requested to:
Restricted Data ☐ Yes ☐ No
Other classified info ☐ Yes ☐ No

CERTIFICATION FOR PERSONNEL HAVING DOD CLEARANCE

This certifies that the person(s) named above needs this access in the performance of duty and that permitting the above access will not endanger the common defense and security.

Authorized access to Critical Nuclear Weapon
Design Information (CNWDI) in Accordance
with DOD Directive 5210.2 ☐ Yes ☐ No **← FILL IN**

LEAVE BLANK
Name and Title, Requesting DOD Official

LEAVE BLANK
Title, Authorizing DOD Official
(See DOD Directive 5210.2 and 5210.8)

LEAVE BLANK
Signature
(See AR 380-180; OPNAV 5510.3F; AFR 2105-1)

CERTIFICATION FOR PERSONNEL HAVING DOE CLEARANCE

This certifies that the person(s) named above needs this access in the performance of duty.

Title Requesting DOE or Other Government Agency

Approval is granted with limitations indicated below:

Manager of Operations for Headquarters Division Director

SEE REVERSE OF PART B FOR PRIVACY ACT INFORMATION STATEMENT

24 MAY 1991

CHAPTER 15

INDUSTRIAL SECURITY

1501. GENERAL

The security of the United States depends in part upon proper safeguarding of classified information released to industry. Classified information (TOP SECRET, SECRET, CONFIDENTIAL) is, and remains for the duration of the classification, the property of the U.S. Government. It may be provided to private industry only in connection with a bona fide contractual requirement. Prior to a contractor having access to classified information, a Security Agreement (DD Form 441) is executed between the Government and the contractor. This Agreement, among other things, requires the contractor to protect classified information per the requirements of the Industrial Security Manual (ISM) (DoD 5220.22-M) of March 1989 (NOTAL), and it requires the Government to specifically identify, in writing, what information will require protection during the contract performance. The ISM provides the contractor with the minimum safeguarding requirements for classified information; it does not provide security classification guidance. Classification guidance is provided to the contractor in the form of a "Contract Security Classification Specification" (DD Form 254). The DD Form 254, with its attachments, supplements, and incorporated references, is the only authorized means for providing security classification guidance to a contractor in connection with a classified contract. Only the procuring military department may originally classify information. A contractor merely marks and protects that information developed under a contract on the basis of the DD Form 254 issued by the government user agency. The government user agency, (hereafter referred to as UA) is the command which actually conducts the contracting process. The UA is responsible for providing to contractors all security classification guidance necessary to properly classify information and material produced under the terms of the contract. It is essential that comprehensive classification security guidance be furnished to contractors. Overall responsibility for administering the Industrial Security Program is assigned to the Director, Defense Investigative Service.

1502. CLASSIFIED CONTRACT

A classified contract is one which requires or will require access (including oral or visual) to classified information by the contractor or his/her employees in the performance of the

24 MAY 1991

contract. A contract may be classified even though the contract document itself or task is not classified. A DD Form 254 shall be prepared following the provisions of Exhibits 15A and 15B of this chapter by the cognizant technical office for each new procurement request which will result in a classified contract. The DD Form 254 shall not be classified.

1503. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD FORM 254)

1. Each procurement request or other document which requires access to classified information for contractual performance must be accompanied by a Contract Security Classification Specification (DD Form 254). The responsibility of the preparation of this form rests with the office having technical cognizance over the procurement. DD Forms 254 are legal contractual documents and will be signed by the Contracting Officer's Technical Representative (COTR) and either OP-09B31 or OP-09B31C, who are designated as Contracting Officers for Security Matters.

2. Cognizant technical offices will prepare a draft DD Form 254 following the instructions provided in Exhibits 15A and 15B, forward this draft, the Statement of Work, and classification guides to OP-09B31C for review, final typing and signature of the Contracting Officer for Security Matters.

3. The cognizant technical office will review the DD Form 254 biennially, as well as whenever classification guidance changes. Results of these reviews will be furnished to OP-09B31C. Biennial review and/or final DD Form 254 will not be required when the contract provides access only to classified information/material or the contract is a service type contract. OP-09B31C will notify cognizant technical offices when contracts are due for review.

4. When final delivery of the end item has been completed and retention of classified material is requested, a final DD Form 254 will be prepared by OP-09B31C. OP-09B31C will be responsible for coordinating requests for retention of classified material, verification of "need-to-know" and any other security or security classification matter. Replies to the requestor will be prepared by OP-09B31C and a copy will be sent to the cognizant technical office.

24 MAY 1991

1504. CLASSIFIED VISITS TO OPNAV/SECNAV/DON STAFF OFFICES BY CONTRACTOR PERSONNEL

1. Refer to Chapter 14 for policy regarding classified visits by contractor personnel.
2. Access to Intelligence information will not be authorized unless the following information is included in the visit request:
 - a. The contractor's certification that access to classified intelligence is required for contract performance and the contract is a classified contract, and;
 - b. Sufficient additional information concerning classified intelligence required to permit the POC to assess the applicability of available classified intelligence to the needs of the contractor and whether available intelligence may be released to the contractor without permission of the originator and/or sanitation of the material, and;
 - c. Certification by the contracting UA activity representative authorized to release classified intelligence to contractors, that the information to be acquired during the visit is not available within the UA.
 - d. The program or project involved has been specified, the level of information to be released is specified, certification from the UA that the visitor has been authorized access to such information and the identity of the office or UA activity granting such authorization.

NOTE: A contractor-granted CONFIDENTIAL clearance (Company CONFIDENTIAL) is not valid for access to RESTRICTED DATA; FORMERLY RESTRICTED DATA; any COMSEC information; SENSITIVE COMPARTMENTED INFORMATION; ACDA (U.S. Arms Control and Disarmament Agency) classified information; NATO information (except for NATO RESTRICTED information); to meet the Personnel Security Clearance (PCL) requirement as a prior condition for certification to fill a Critical or Controlled Position under the Nuclear Weapon Security Program; classified foreign government information; or for assignment to duty stations outside the U.S.

3. If access to classified information requiring a special access authorization (i.e., NATO, military space project or other special or limited access programs), the request will, in addition to the other required information:

24 MAY 1991

- a. Specify the program or project,
- b. Specify the level of information to be released,
- c. Certify from the UA that the visitor has been authorized access to such information, and
- d. Provide identity of the office or UA activity granting such authorization.

4. If contract performance is to be in whole or in part onsite (within office spaces), obtain approval of OP-09B31 to ensure that all security requirements are addressed. Contractor employees are not attached to the command, therefore do not come under administrative control of the command. Any security issues pertaining to on-site contract performance must be included in the DD Form 254 for the contract and any supplemental security requirements appended. Refer to Item 15 of Exhibits 15A and 15B, and Exhibit 15C.

1505. DISSEMINATION OF CLASSIFIED MATERIAL TO DOD CONTRACTORS

1. Classified material will only be disseminated to contractor personnel as outlined in this chapter and Chapter 9.

2. Policy regarding the handcarrying of classified material by contractor personnel out of OPNAV/SECNAV/DON Staff Office spaces is contained in Chapter 6.

3. All classified material to be forwarded to contractors will be processed through the Correspondence Control, Mail and Files Branch (OP-09B34) or NATO Subregistry/Top Secret Control Unit (OP-09B31C2) as applicable to the type of material being transmitted.

4. Classified material must be sent with a letter of transmittal and an Outgoing Mail Record (OMR). The letter of transmittal will contain the contract number under which the classified material is being released. In addition the releasing office will certify that verification of the Facility Clearance, Safeguarding Capability and correct classified mailing address of all addresses has been obtained as outlined in paragraph 1012 of this instruction.

5. Access to classified information by a contractor is normally justified when:

24 Mar 1991

a. A bona fide contractual relationship exists between the contracting organization and an element of the DOD, or

b. Access is required in connection with precontract negotiations, and

c. The organization has a current facility clearance commensurate with the classification of the information to which access is requested, and

d. The person(s) for whom the access authorization is intended have a personnel security clearance commensurate with the information to which access is requested, and

e. The person(s) for whom access is requested has a valid "need-to-know".

1506. PROCEDURES FOR ISSUE OF DOD BUILDING PASSES TO CONTRACTOR PERSONNEL

The policies and procedures regarding the issuance of DOD Building Passes to contractor personnel are contained in Chapter 3.

1507. CONSULTANT CLEARANCES

1. The information contained in this section refers to those consultants hired under the provisions of the Office of Personnel Management but are not paid. Consultant clearances will not be processed unless the consultant is approved and processed via the civilian personnel office.

2. In all cases, personnel security clearances/facility security clearances/classified storage capability for self-employed consultants, shall be processed in accordance with the provisions of the Industrial Security Regulation (DOD 5220.22-R) of March 1989 (NOTAL) and the following:

a. **Type A** - The consultant does not possess classified material, except at the user agency activity or while on authorized visits to another government agency/cleared contractor facility. The consultant, for security administrative purposes only, shall be considered to be an employee of the user agency.

b. **Type B** - the consultant possesses classified material at his/her place of business or residence, the consultant having full responsibility for the security of the classified material. The processing of a facility security clearance/request for

24 MAY 1991

classified storage capability is required for Type B consultants to cover the premises at which he/she will possess the classified material and perform the consulting services. Type B consultants shall be considered to be prime contractors to the user agency. The execution of a DD Form 254 is required. Refer to Exhibits 15A and 15B for instructions in the preparation and use of DD Form 254.

c. Type C - The consultant possesses classified material at his/her regular employer's cleared facility, the consultant and his/her employer having agreed as to their respective responsibilities for security of the classified material. A copy of this agreement must be on file with OP-09B31.

3. Type A, B and C consultant clearances will be processed by OP-09B31C. Requests shall be submitted to OP-09B31C from Secretariat, Headquarters Civilian Personnel Office (S/HCPD) as for all other civilians hired. Applicable forms required for processing type A, B and C consultant clearances will be disseminated by OP-09B31C upon approval of request. DO NOT SUBMIT INVESTIGATIVE/CONSULTANT AGREEMENT FORMS THAT WERE NOT PROVIDED FOR SUCH PURPOSES BY OP-09B31C.

4. Access to classified information will not be granted to consultants until a Letter of Consent (DISCO Form 560) has been issued to OP-09B31C by the Defense Industrial Security Clearance Office (DISCO). Although a prospective consultant may have a current valid clearance with a DOD contractor, it is not valid for use as an OPNAV, SECNAV or DON Staff Office consultant. A concurrent clearance must be obtained through OP-09B31C from DISCO.

5. Security Coordinators are responsible for ensuring that consultants check-out with OP-09B31. Check-out procedures will consist of return of passes and written verification from the cognizant Security Coordinator that the consultant has been debriefed and if applicable, all classified material has been turned in to the employing office. OP-09B31C will execute a Personnel Security Clearance Change Notification (DISCO Form 562) or execute a final DD Form 254 to administratively terminate the individual's clearance.

24 MAY 1991

EXHIBIT 15A

PROCEDURES AND GUIDELINES ON PREPARATION OF DD FORM 254

Early in the acquisition cycle, certain security requirements must be considered. Will access to classified information be involved? Will access be required during the pre-award phase, or will it only be required for actual performance of the contract? Are all the prospective contractors cleared to the appropriate level, and are they equipped to properly safeguard the classified information involved? The answers to these questions and the timeliness of your action will have a significant impact on your acquisition and the Defense Industrial Security Program (DISP). Enough lead time in your acquisition cycle should be provided to accomplish the security actions that may be needed. In many instances, advanced planning can ensure that the bid package will not require access to classified information, and prevent processing an entire bidders list for facility security clearances. When access is required in the pre-award phase, an interim facility security clearance may be the solution. If access is not a factor in the pre-award phase, but will be required for contract performance, only the successful bidder will be processed for a facility clearance. Processing unnecessary prospective contractors for facility clearances is very time consuming, costly and greatly increases the time it takes to process that one contractor who actually has a need for a clearance. First you must determine the security requirements for the proposed contract:

Access to classified information will be required. This is a "classified contract" within the meaning of the Industrial Security Program. Certain security clauses must be incorporated in the solicitation and in the contract, and certain security clearances will be required.

Access will not be required in the pre-award phase. Prospective contractors do not have to possess facility security clearances to bid on the solicitation. Only the successful bidder must have an appropriate facility security clearance, and safeguarding capability, if required.

Access will be required during the pre-award phase. All prospective contractors must possess the appropriate facility clearance and safeguarding capability if they will possess any classified information during this phase.

24 MAY 1991

After you have decided the security requirements you must determine the current clearance status of all prospective contractors:

All prospective contractors have appropriate clearance. No further clearance action is needed.

Some prospective contractors do not have appropriate clearances. All prospective contractors must have an appropriate clearance prior to release of the information. A request must be submitted to the Cognizant Security Office (CSO) furnishing the appropriate information needed to process the clearance.

The next step is to determine what security classification guidance the contractor will need to perform on the contract. A "Contract Security Classification Specification" (DD Form 254) is required for each classified contract and must be incorporated in the solicitation and in the contract. Even if pre-award access is not required, the DD Form 254 should be incorporated in the solicitation to provide the contractor with information needed during contract performance. If pre-award access is not required, add the following notation in Item 11o. "Remarks" of the DD Form 254. "Pre-award access is not required. This DD Form 254 reflects the security requirements for the contract when awarded."

The DD Form 254, issued with the solicitation (RFQ, RFP, or IFB), is always an "original." When the contract is awarded and the contract number is assigned, another "original" DD Form 254 is issued reflecting the contract number and date of issuance. The following correspond to the numbered items of DD form 254 (see Exhibit 15B):

Item #1:

Insert the highest level of facility clearance required for access to classified information in the performance of the contract. Use only the words TOP SECRET, SECRET, or CONFIDENTIAL. Special caveats such as RESTRICTED DATA, FORMERLY RESTRICTED DATA, CRYPTOGRAPHIC INFORMATION, will not be indicated in this block. The facility security clearance of the contractor shown in Item 7a must be at least as high as the classification indicated in this block. If the level of safeguarding required for performance is less than the facility clearance required, add a statement in Item 15 indicating the appropriate safeguarding level.

24 MAY 1991

Item #2:

For the actual contract when awarded, place an "X" in Item 2a, or for an RFP, RFQ, or IFB place and "X" in Item 2c.

Item 2b, for subcontractor DD Forms 254 is normally completed by the prime contractor.

Item #3:

For Item 3a, when the actual contract has been awarded, enter the Contract Number, or for an RFP, RFQ, or IFB enter the procurement Request Number in Item 3c.

Item 3b, for subcontractor DD Forms 254 is normally completed by prime contractor.

Item #4:

For Item 4a, indicate estimated contract completion date. The date given is used to update security guidance at fixed periods in conformance with DoD regulations. Obviously, the date given should be as close an approximation as possible, or

For Item 4c, the due date of the RFP, RFQ, or IFB shall be entered.

Item 4b, for subcontractor DD Form 254 is normally completed by prime contractor.

Item #5:

Place an "X" in Item 5a for original RFP, RFQ, or IFB DD Form 254 or for original DD Form 254 when contract is awarded and the date of preparation. The date of the original DD Form 254 prepared when the contract is actually awarded will appear unchanged on each revised and final DD Form 254.

Place an "X" in Item 5b only when revising an existing DD Form 254. Each time a revision is made, it will be given a revision number and date of revision. The original is revision 0 and each revision thereafter is given a sequential number.

Place an "X" in Item 5c when preparing a final DD Form 254 upon contract completion and the date of preparation.

24 MAY 1991

Item #6:

This Item pertains to follow-on prime contracts. It must be to the same prime contractor for the same item(s) or services, with no changes in the security classification guidance applicable to the contract. When these conditions exist, enter an "X" in the "Yes" box, and enter the number and completion date of the preceding contract in Items 6a and 6b. In Item 6c, enter an "X" in the "Is" box. In all other cases,, enter an "X" in the "No" box. This is an important Item because it authorizes the contractor to transfer accountability of classified material from the preceding contract to the current one. It eliminates the need for the contractor to request retention of the classified material until completion of the current contract. **NOTE:** Intelligence material shall not be transferred to another contract.

Item #7:

If requesting a sole source procurement, enter the contractor's name and address in Item 7a. If requesting a competitive procurement, leave Item 7a blank. If the actual work is to be performed at a location other than that shown in Item 7a, identify the work location in Item 15. OP-09B31C will verify the cleared classified mailing address for contractors, and will complete Items 7b and 7c.

Item #8:

Insert N/A. This Item is not applicable for a prime contract.

Item #9:

Insert N/A. This Item is not applicable for a prime contract.

Item #10:

Item 10a - Enter a description of the procurement. This may be material, studies, services, etc. The statement should be short, concise, and unclassified.

Item 10b - Is the Department of Defense Activities Address Directory (DoDAAD) number of the Procuring Activity.

Item 10c - Indicates whether or not the procurement will require security measures that are additional to those normally required in the ISM, such as access to Sensitive Compartmented Information

24 MAY 1991

or other special access programs; if contract performance is required outside the U.S., its possessions or dependencies; if contract performance requires unique or special facilities or locations for security purposes; or if access to Intelligence Information is required.

The release of Intelligence Information to contractors must be in accordance with Chapter 12, paragraph 12-21.4, of OPNAVINST 5510.1H. This must be specifically authorized in the DD Form 254 for the contract, by reference in item 15 and attaching an Intelligence Information Sheet. Check with OPNAV Security or the Contracting Officer for Security of the contracting agency.

Item 10d - Check "Yes" only if the procurement requires access to Sensitive Compartmented Information (SCI) or other Special Access Program (SAP) information and there are areas or elements outside Defense Investigative Service security cognizance. Identify specific areas or elements in Item 15.

Item #11:

Check "Yes" or "No" for each Item to define specific contractor access limitations. Contractors may not receive information unless specifically authorized by these Items.

Item 11a - Access to Classified Information only at other contractor/government facilities. Note the word "only". If the "Yes" box is marked for this Item, Items 11b thru 11e plus Items 11m and 11n must be marked "No" and the remaining Items marked as required. The contractor will not be required to have any safeguarding capability at his facility if this Item is marked "Yes". The following notation shall be added in Item 15:

"Using Government activity will furnish complete classification guidance for the service to be performed. Contract performance is restricted to (name of contractor or Government activity and location)."

Item 11b - Receipt of Classified Documents or Other Material for Reference Only (No Generation). Note the word "only". If the "Yes" box is marked for this Item, Items 11a, 11c thru 11e, and 11n must be marked "No" and the remaining Items marked as required. The contractor will be required to have safeguarding capability at his facility.

24 MAY 1991

Item 11c - Receipt and generation of Classified Documents or Other Material. If the "Yes" box is marked for this Item, Items 11a, 11b and 11e must be marked "No" and the remaining Items marked as required. The contractor will be required to have safeguarding capability at his facility.

Item 11d - Fabrication/Modification/Storage of Classified Hardware. If applicable, include as much information as possible (additional information can be added in Item 15) to indicate if Restricted or Closed Areas will be required. How much hardware is involved? How large? When does the hardware become classified?

Item 11e - Graphic Arts Services Only. Note the word "only". If the "Yes" box is marked for this Item, Items 11a thru 11d must be marked "No" and the remaining Items marked as required. This type of contract would not require any specific classification guidance because the markings on the documents provided would be sufficient guidance for the contractor. The contractor will be required to have safeguarding capability at his facility. The following notation will be added in Item 15:

"Reproduction service only. Classification markings on the material to be reproduced specify the required guidance."

Item 11f - Access to IPO Information. This means International Pact Organizations such as NATO. Permission of the prime contracting officer is required prior to subcontracting.

Item 11g - Access to RESTRICTED DATA. This Item includes access to FORMERLY RESTRICTED DATA and CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI) and is information developed and controlled under the Atomic Energy Act of 1954. Note this Item would always be marked "Yes" if access to CNWDI is required. Permission of the prime contracting officer is required prior to subcontracting if CNWDI access is involved. Item 11o or Item 15 should contain a statement such as, "Access to CNWDI is required."

Item 11h - Access to Classified COMSEC Information. This Item pertains Communications Security Information such as COMSEC equipment, materials, information or manuals. Special briefings, markings, and controls are required. If a COMSEC account is required, so state in Item 11o "Remarks." Permission of the prime contracting officer is required prior to subcontracting.

Item 11i - Cryptographic Access Authorization Required. This Item no longer applies. Mark it N/A.

24 MAY 1991

Item 11j - Access to Sensitive Compartmented Information (SCI). If this information is involved, the Special Security Officer (SSO) should be contacted prior to any contracting. Special security measures are required. Ensure that Items 10c and 10d are appropriately checked and the additional information is included in Item 15. The following statement will also appear in Item 15 when SCI is required: "This contract requires access to SCI. The (enter appropriate Agency/Military Department SSO) has exclusive security responsibility for all SCI classified material released to or developed under the contract and held within the contractor SCIF. DIS is relieved of security/inspection responsibility for all such material but retains responsibility for all non-SCI classified material released to or developed under the contract and held within the contractor SCIF." Additional guidance for physical, personnel, and information security measures would be incorporated into the contract or provided by other means. A copy of the DD Form 254 must be forwarded to the Agency/Military Department that will have security responsibility.

Item 11k - Access to other Special Access Program Information.

These types of programs usually require additional security procedures or actions. These requirements are varied and may be different for each type of Special Access Program. Additional information must be included in Item 15. Item 10c and/or Item 10d may also apply for these programs.

Item 11l - Access to U.S. classified information outside the U.S., Panama Canal Zone, Puerto Rico, U.S. possessions and trust territories. If "Yes", indicate city and country of overseas performance in Item 15. A copy of the DD Form 254 must be provided to the U.S. activity responsible for overseas administration.

Item 11m - Defense Documentation Center (DDC) Services may be requested. DDC is now the Defense Technical Information Center (DTIC). "Yes" in this Item will require that a DD Form 1540 and DD Form 1541 be prepared and processed by the contractor before he may request these services. The DD Form 1540 (Registration for Scientific and Technical Information Services) must be submitted to the Contracting Agency for validation of the contractor's "Need-to-Know."

Item 11n - Classified ADP Processing will be involved. This Item will be marked "Yes" if processing classified information will be required at the contractor's facility or at the User Agency. It

24 MAY 1991

does not apply if the contract is for maintenance service. If this Item is marked "Yes", the contractor will be required to prepare an ADP/SPP for his/her ADP operations and the system will require approval of the Cognizant Security Office in accordance with Section XIII, ISM. ADP processing refers to computers, word processors, etc. If classified ADP processing at the User Agency is involved or unclassified processing at the User Agency or contractor facility, the contractor must comply with the User Agency ADP Security Regulations. Address these instances in Item 15 and provide the contractor with a copy of such regulations as an attachment to the DD Form 254. The Command ADP Security Officer will review all drafts where this item is marked "yes".

Item 11o - Remarks. This Item may be used for any other pertinent information.

Item #12:

This is a statement of completeness and adequacy of the DD Form 254 that is being signed by the individual named in Item 12b.

Item 12a - No entry required.

Item 12b - The typed name, title and signature of the Program/Project Manager.

Item 12c - The typed complete mailing address, including ZIP code, commercial telephone number (including Area Code), office code symbol and autovon telephone number of the individual named in Item 12b.

Item #13:

This Item concerns the contractor's public release of any information under the contract. The contractor is responsible for obtaining the approval of the contracting officer for the prime contract.

Item 13a - Appendix IX no longer applies to public release. Please delete.

Item 13b - Insert an "X" in block, then insert "Chief of Naval Operations, OP-09B31, Department of the Navy, Washington, DC 20350-2000. If NO PUBLIC RELEASE AUTHORIZED, so state.

source documents be provided. Do they contain all the guidance the contractor needs? Will classified hardware be furnished or produced by the contractor? What information makes the hardware classified? At what stage in its production does it become classified? What unique characteristics are involved that need protection? What technical information requires protection? What breakthroughs would be significant if achieved in an R&D effort? Are there performance limitations that require protection? These are merely some of the questions you should ask when preparing your guidance for a contract. Put yourself in the contractor's place and try to determine what guidance will be needed to properly protect the classified information that will be furnished or generated under the contract. Give reasons for

24 MAY 1991

the classification. Write the guidance in plain English. Don't try to follow a format or provide all the guidance in this block.

Each contract is unique in its performance requirements. "Boilerplate" guidance should be avoided. Use this block to identify applicable guides, to provide narrative guidance which identifies the specific types of information to be classified and appropriate downgrading or declassification instructions, to show any special instructions, and to provide any explanatory comments or statements required for information or clarification of other items identified in the DD Form 254. Expand as necessary by adding additional pages.

The DD Form 254, with its attachments and incorporated references, is the only authorized means for providing security classification guidance to a contractor. It should be written as specific as possible and it should include only that information that pertains to the specific contract. It should not contain reference to your internal agency directives and instructions. If these documents provide guidance applicable to the performance of the contract, the pertinent portions should be extracted and provided with the DD Form 254. (Note: This information is very important when contract performance is to be in whole or in part on-site. See also Exhibit 15C.) Any and all documents referenced in a DD Form 254 should be provided to the contractor, either as an attachment or forwarded under separate cover if they are classified. The requirements of the ISM should not be included in a DD Form 254; the ISM contains safeguarding requirements and procedures, not security classification guidance.

Writing security classification guidance covering the performance requirements of a classified contract can be very difficult to accomplish to be understood and implemented in a contractor's environment. The contractor should be encouraged to assist in preparation of the guidance, if at all possible, and to provide comments and/or recommendations for changes in the guidance that has been provided. Only through effective communication with the contractor can guidance be achieved that is understandable and will ensure the proper classification of the information generated in the performance of the contract.

Guidance will normally include one or more of the following:

(1) Identify security classification guides or extracts thereof which are furnished to the contractor. (Refer to OPNAVINST 5513 series of security classification guides - ensure specific enclosure(s) number(s) which apply have been indicated.)

24 MAY 1991

(2) Narrative classification guidance if necessary, which identifies the specific types of information to be classified and appropriate downgrading and/or declassification instructions. When classified hardware is part of the contract, identify the classified hardware and indicate when the hardware becomes classified, if possible.

(3) Any special instructions and controls for handling, processing, storing, and transmission of the classified material.

(4) Any explanatory comments or statements required for information or clarification of other Items identified in the DD form 254.

(5) When the contract is for certain types of services and Item 14c is marked, specific statements must appear in this Item. OP-09B31C will assist in addressing the proper statements.

(6) Locations where work will be performed if different from the address shown in Item 7a. This will also apply if contract performance is to be in whole or in part on-site. (See also Exhibit 15C.) Additional security guidance may be required as an attachment to the DD Form 254 for on-site contract performance. The contractor is not responsible for compliance with command security procedures (to include ADP Security requirements) unless addressed in the DD Form 254 or attachments.

(7) Special restrictions on release of and access to classified material.

This Item may be expanded as necessary by adding additional pages as necessary.

Item #16:

To be completed by the Contracting Officer for Security.

Required Distribution for Prime Contracts.

- (1) Prime contractor
- (2) CSO of prime contractor only
- (3) Appropriate ACO
- (4) Quality assurance representative
- (5) Official identified in Item 12b, DD Form 254
- (6) OP-09B31C
- (7) Others as necessary

24 MAY 1991

EXHIBIT 15B

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(DD FORM 254)**

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION		THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: SECRET	
2. THIS SPECIFICATION IS FOR		3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER (Prime contracts must be shown for all subcontracts)	4. DATE TO BE COMPLETED (Estimated)
X A. PRIME CONTRACT		a. PRIME CONTRACT NUMBER N00014-89-C-0000	b. DATE TO BE COMPLETED 30 SEP 90
D. SUBCONTRACT (See item 15 for subcontracting beyond second tier)		d. FIRST TIER SUBCONTRACT NO.	e. THIS SPECIFICATION IS: (See "NOTES" below. If from A or C is "X", also enter date for item e)
E. REQUEST FOR BID REQUEST FOR PROPOSAL OR REQUEST FOR QUOTATION		e. IDENTIFICATION NUMBER	f. DATE 30 SEP 89
6. Is this a follow-on contract? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. IF YES complete the following:		g. REVISION (Indicate all previous specifications)	
a. N00014-86-C-0000		h. REVISION NO.	
b. 30 SEP 89		i. DATE	
c. ACCOUNTABILITY for classified material on preceding contract		j. FINAL	
X Is not transferred to this follow-on contract		k. DATE	
7a. Name, Address & Zip Code of Prime Contractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
ABC Incorporated 123 Any Street Washington, DC 20000-0000		0X000	Defense Investigative Service Director of Industrial Security 2461 Eisenhower Avenue Alexandria, VA 22331-1000
8a. Name, Address & Zip Code of First Tier Subcontractor *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
N/A		N/A	N/A
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *		b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
N/A		N/A	N/A
10a. General Identification of the Procurement for which this specification applies		b. DoDAB Number of Procuring Activity identified in item 10a	
UNCLASSIFIED DESCRIPTION OF PROCUREMENT		N00014	
c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No. IF YES, identify the pertinent contractual documents in item 15			
d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No. IF YES, explain in item 15 and identify specific areas or elements			
11. ACCESS REQUIREMENTS		YES	NO
a. Access to Classified Information Only at other contractor/Government activities		X	
b. Receipt of classified documents or other material for reference only (no generation)		X	
c. Receipt and generation of classified documents or other material		X	
d. Fabrication/Minification/Repair of classified hardware		X	
e. Graphic arts services only		X	
f. Access to IPO information		X	
g. Access to RESTRICTED DATA		X	
h. Access to classified COMSEC information		X	
i. Cryptographic Access Authorization required		X	
12. Refer all questions pertaining to contract security classification specification to the official named below (NORMALLY, thru ACO (item 10a); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontractors):		j. ACCESS REQUIREMENTS (Continued)	
a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate		1. Access to SENSITIVE COMPARTMENTED INFORMATION	
b. Typed name, title and signature of program/project manager or other designated official		2. Access to other Special Access Program Information (Specify in item 15)	
SEE INSTRUCTIONS		3. Access to U. S. classified information outside the U. S., Panama Canal Zone, Puerto Rico, U. S. Possessions and Trust Territories	
NOTE: Original Specification (Item 1a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.		4. Defense Documentation Center or Defense Information Analysis Center Services may be requested	
		5. Classified ADP processing will be involved	
		6. REMARKS:	
		Item 10.c=Access to Intelligence Information required. See item 15.	
		Item 11.g=Access to CNWDI required.	
		Item 11.n=DIS approved equipment only.	
		7. PROGRAM/PROJECT MANAGER'S COMPLETE MAILING ADDRESS, AREA CODE WITH PHONE NUMBER, AND AUTOVON NUMBER.	

DD FORM 254
1 JAN 79

EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254, WHICH IS OBSOLETE.

B/N 0102-LF-000-2540

24 MAR 1991

EXHIBIT 15B

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(DD FORM 254)

<p>13a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual (paragraph 5a and Appendix 1X).</p>	
<p>b. Proposed public releases shall be submitted for approval prior to release. <input type="checkbox"/> Direct <input checked="" type="checkbox"/> Through (Specify): Chief of Naval Operations (OP-09B31), Department of the Navy, Washington, DC 20350-2000. to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) * for review in accordance with paragraph 5a of the Industrial Security Manual. <small>* In the case of non-DoD User Agencies, see footnote, paragraph 5a, Industrial Security Manual.</small></p>	
<p>14. Security Classification Specifications for this solicitation/contract are identified below ("X" applicable boxes) and equity attachments as required. Any narrative or classification guideline furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guideline is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in item 14b. The following information must be provided for each item of classified information identified in an extract or guide: (I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading (if applicable). The official named in item 12b is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.</p>	
<p><input checked="" type="checkbox"/> a. A completed narrative is (1) <input checked="" type="checkbox"/> See item 15 transmitted under separate cover and made a part of this specification. <input checked="" type="checkbox"/> b. The following classification guideline is made a part of this specification and is (1) <input type="checkbox"/> attached, or (2) <input checked="" type="checkbox"/> transmitted under separate cover. (List guideline under item 15 or in an attachment by title, reference number and date). <input type="checkbox"/> c. Provide type contract/subcontract. (Specify instructions in accordance with ISIR/ISN, as appropriate). <input type="checkbox"/> d. "X" only if this is a final specification and item 6 is a "NO" answer. In response to the contractor's request dated _____, revision of the identified classified material is authorized for a period of _____. <input checked="" type="checkbox"/> Biennial review of this DD Form 254 is required. If "X'd" provide date such review is due: 30 SEP 91</p>	
<p>15. Remarks (Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions). 1. Document preparation and distribution shall be only as prescribed by the Contracting Officer's Technical Representative (COTR). The COTR is responsible for reviewing all material in draft form, determining proper classification, and affixing all final classification authority/declassification markings. 2. Information generated under this contract shall be marked in accordance with the provisions of the Industrial Security Manual for Safeguarding Classified Information (DOD 5220.22-M). 3. Classified material generated by the contractor under this contract shall be classified by: (fill in applicable classification guide(s)), which will be provided to the contractor by the Program Manager/Project Officer under separate cover. 4. An Intelligence Information Sheet is provided as enclosure (1) to this DD Form 254, and is hereby made a part of this contract. 5. Any subcontract DD Form 254's issued incident to this contract and all certifications of "Need-to-Know" in connection with this contract, must be approved by the official shown in item 16.b below.</p>	
<p>16. Contract Security Classification Specifications for Subcontractors issuing from this contract will be approved by the Official named in item 16a below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the User Agency Contracting Officer or his Representative named in item 16b below.</p>	
<p>REQUIRED DISTRIBUTION:</p> <p><input checked="" type="checkbox"/> Prime Contractor (from 7a) <input type="checkbox"/> Cognizant Security Office (from 7c) <input checked="" type="checkbox"/> Administrative Contracting Office (from 16a) (optional) <input type="checkbox"/> Quality Assurance Representative <input type="checkbox"/> Subcontractor (from 8a) <input type="checkbox"/> Cognizant Security Office (from 8c) <input checked="" type="checkbox"/> Program/Project Manager (from 12b) <input type="checkbox"/> U. S. Activity Responsible for Overseas Security Administration</p> <p>ADDITIONAL DISTRIBUTION:</p> <p><input checked="" type="checkbox"/> CNR Codes 00R11 & 1514 <input checked="" type="checkbox"/> CNO OP-09B31C <input type="checkbox"/></p>	<p>b. Typed name and title of approving official (LEAVE BLANK)</p> <p>c. Signature (LEAVE BLANK)</p> <p>d. Approving official's activity address and Zip Code (LEAVE BLANK)</p> <p>e. Name, address and Zip Code of Administrative Contracting Office (optional)</p>

24 MAY 1991

EXHIBIT 15B

**INTELLIGENCE INFORMATION SHEET
(SUPPLEMENTAL ATTACHMENT TO DD FORM 254)**INTELLIGENCE INFORMATION SHEET

1. Intelligence material provided to the contractor does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all Intelligence released and any material using data from such Intelligence will be returned to the Contracting Officer's Technical Representative (COTR) for final disposition. Only with prior written authorization from the Chief of Naval Operations (OP-09B31), Department of the Navy, Washington, DC 20350-2000, may the contractor retain such material.
2. Contractors will not release the Intelligence material to any activity or person of the contractor's organization not directly engaged in providing services under the contract or to another contractor (including sub-contractors), government agency, private individual, or organization without prior written approval of the Chief of Naval Operations (OP-09B31), Department of the Navy, Washington, DC 20350-2000.
3. Intelligence material will not be released to foreign nationals or immigrant aliens who may be employed by the contractor, regardless of the level of their security clearance or access authorization, except with the specific written permission of the Chief of Naval Operations (OP-09B31), Department of the Navy, Washington, DC 20350-2000.
4. Intelligence material will not be reproduced without prior written approval from the Chief of Naval Operations (OP-09B31), Department of the Navy, Washington, DC 20350-2000. All Intelligence material will bear a prohibition against reproduction while in the custody of the contractor.
5. The contractor will maintain records which will permit them to furnish, on demand the names of individuals who have access to Intelligence material in their custody.

CONTRACT NUMBER: N00014-89-C-0000
DD 254 DTD: 30 SEP 89
ENCLOSURE (1)

24 MAY 1991

EXHIBIT 15C

GUIDELINES FOR ON-SITE CONTRACT PERFORMANCE

1. Before initiating any procurement action requiring contract performance to be in whole or in part on-site, (within office spaces), approval must be obtained from OP-09B31 via OP-09B31C to ensure that all security requirements are addressed. Provide OP-09B31C with copies of the "Statement of Work" and your rough draft DD Form 254. Contractor employees are not attached to the command, therefore do not come under administrative control by any authority within the command. However, by including applicable requirements in the DD Form 254, we can commit the Navy and hold the contractor facility responsible for items which are covered. Security requirements may also increase the contract costs, so do not unnecessarily include security items that need not be performed by the contractor. Having contractor employees on access lists and acting as custodians for classified material/spaces is not encouraged and must only be requested when contract performance cannot be achieved by any other means.

2. Once it has been determined that contract performance must be conducted on-site and the contractor(s) must be responsible for some security aspects, this will be included in the DD Form 254 in item 15 "Remarks" and any applicable additional security regulations, procedures, instructions, etc., must become an enclosure or attachment to the DD Form 254. This is the only way to enforce the security requirements. A contractor employee cannot be responsible for securing a classified container unless it has been put in writing and applicable security guidance regarding such actions has been provided. The most common instance for which contractor employees will be required to perform on-site is when ADP support of some type is to be performed by the contractor. In these cases, the command ADP Security Program must apply to the contractor also and be addressed in the DD Form 254, otherwise there has been no commitment by the contracting facility to comply with any command security policies regarding ADP Security.

3. In addition to including the on-site performance requirement in the DD Form 254, the following items must be considered and executed as applicable on a case-by-case basis:

- a. Provide the contractor written instructions specifying:

24 MAY 1991

(1) Those security actions (if any) which will be performed for the contractor by the installation such as providing storage facilities, guard service, mail and freight services, visit control, and;

(2) Those security actions (if any) for which joint action may be required such as the packaging and addressing of classified transmittals, and control of visitors.

b. Ensure that the contractor has prepared a Standard Practice Procedure (SPP) covering the contractor's activities on the installation, if appropriate.

c. Ensure that the contractor observes required security controls through periodic inspections in accordance with the schedule prescribed by paragraph 4-103 of the Industrial Security Regulation (ISR, DoD 5220.22-R) of December 1985 (NOTAL), and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

d. Ensure that prompt remedial action is taken when security conditions are deficient in the contractor's operations.

e. Ensure that the DoD Security Education Program is implemented by the contractor and, as required, conduct defensive security briefings required by paragraph 5u of the Industrial Security Manual for Safeguarding Classified Information (ISM, DoD 5220.22-M) of March 1989 (NOTAL).

f. Conduct investigations of contractor security violations, including loss, compromise, or suspected compromise of classified information.

g. Conduct the briefing and debriefing of the Facility Security Officer (FSO), the COMSEC custodian, and alternate COMSEC custodian when there is a COMSEC account or there is a requirement to establish a COMSEC account (see also paragraph 2-313 of the ISR). Brief and debrief only the FSO if no COMSEC account is required.

h. Furnish to the contractor guidance on the application of security requirements to the contractor's operations.

i. Forward requests from the contractor for interpretations of the ISM to the Cognizant Security Office (CSO).

24 MAY 1991

j. Request interim PCL's from DISCO for contractor personnel, when required, to prevent crucial delay in the performance of the contract.

k. Ensure that the contractor reports promptly any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information. In addition, the CSO of the visiting contractor's facility shall be advised concerning the incident.

4. The Standard Practice Procedure (SPP) will include in sufficient detail to place into effect all security controls required in addition to the ISM which are applicable to the contract on-site operation.

5. Normally all defensive security briefings will be provided to the contractor (e.g. orientation, refresher, counterespionage, etc.) by their contractor facility. However, when required for unique training applicable to only the contractor employee(s) performing contract work on-site, briefings may be provided by the installation. In any case, if the on-site contractor employee requires a foreign travel briefing, the installation must be notified by the contractor facility for record purposes even though the contractor facility will be providing the briefing to the employee.

6. The purpose of these guidelines, is when required, to have a contractor employee responsible to applicable security regulations, policies, instructions, when they must perform a security function on-site in the same manner in which an employee would. Remember this is not encouraged and should only be requested when no other alternative exists to enable contract performance.

CHAPTER 16

COMPROMISE AND OTHER SECURITY VIOLATIONS

1601. GENERAL

1. It is the duty of each person in the Department of the Navy to comply with the provisions of Chapter 4 of reference (a), particularly as they relate to the reporting of loss, possible loss, or subjection to compromise of classified information. Reports of loss, possible loss, compromise, possible compromise and violations of security regulations must be reported to the OPNAV Security Manager (OP-09B31). Individuals should make such reports to Directorate Security Coordinators who will inform the OPNAV Security Manager (OP-09B31).

2. There are two types of security violations: one which results in compromise or a possible compromise of classified information; the other which results in security regulations being violated but no compromise occurs.

3. Compromise is the disclosure of classified information to a person who is not authorized access. The unauthorized disclosure may have occurred knowingly, willfully or through negligence. Compromise is confirmed when conclusive evidence exists that classified information has been disclosed to an unauthorized person. A possible compromise is when some evidence exists that classified information may have been subjected to unauthorized disclosure.

4. Compromise presents the greater threat to national security, but other security violations must also be treated seriously because they demonstrate that a weakness exists in a command's security program. For this reason, security violations of either type must be reported, vigorously investigated and corrected rather than covered up. Incidents of an individual's failure to comply with the policies and procedures for safeguarding classified information will be evaluated to determine eligibility to hold a security clearance.

1602. SECURITY VIOLATIONS

1. When the OPNAV Security Manager (OP-09B31) has determined that there has been a security violation, a report of the violation (OPNAV 5511/5) will be sent from the Assistant Vice Chief of Naval Operations (OP-09B) to the ACNO, DCNO, DSO,

14 MAY 1991

Administrative Aide to SECNAV or the principal office of the Navy Staff Office concerned. A preliminary inquiry will be conducted by the appropriate Security Coordinator or other designated official. To avoid a conflict of interest, no individual involved or suspected of involvement with a security violation will be permitted to act as an inquiry official, nor will inquiry report results be reported via any individual involved or suspected with a security violation.

2. Preliminary inquiries will be completed within 3 days from when OP-09B signs the violation report and must:

a. Completely and accurately identify the information lost, compromised or subjected to possible compromise, to include:

- (1) Classification of the material
- (2) All serial numbers
- (3) Date
- (4) Originator
- (5) Subject
- (6) Downgrading/declassification
- (7) Number of pages

b. Determine the circumstances surrounding the incident.

c. Identify all witnesses to the violation and informally interview them to determine the extent of the violation.

d. Identify the individual responsible, if possible.

e. Make an attempt to discover the weakness in security procedures that allowed the compromise or subjection to compromise to occur.

f. Evaluate the information compromised or subjected to compromise to determine the extent of potential damage to national security, and the action necessary to minimize the effects of the damage.

g. Include a statement that the Naval Investigative Service (NIS) field office, Naval Investigative Service Resident Agency (NISRA), Washington Navy Yard, telephone 433-3858) has been advised and accepted or declined investigation responsibility.

24 MAY 1991

h. Establish either:

(1) That an unauthorized disclosure of classified material did not occur (see paragraph 3 below), or the compromise may have occurred but under circumstances presenting a minimal risk to national security (see paragraph 4 below), or

(2) That compromise is confirmed and that the probability of damage to the national security cannot be discounted (see paragraph 5).

3. If it is determined that a compromise or possible compromise in fact did not occur, the inquiry will be terminated and report of inquiry will be sent via the Principal Official to OP-09B.

4. If a determination of:

a. Minimal risk is made,

b. No significant command security weakness is found,
and

c. Formal disciplinary action is not appropriate, then the Principal Official will send the inquiry to OP-09B. If OP-09B agrees that all three conditions have been met, the preliminary inquiry will be returned by endorsement to the appropriate Principal Official advising that notification of the originator of the material involved is required. The Principal Official will notify originators (in DOD) that no further action will be taken with copy to OP-09N and NISRA Washington Navy Yard. OP-09N will notify originators outside DOD.

d. If OP-09B does not agree that the three conditions have been met, a Judge Advocate General (JAG) Manual Investigation will be directed. A copy of the JAG investigation will be sent via OP-09B to OP-09N.

5. If the Principal Official conducting the inquiry determines that:

a. Compromise is confirmed, and

b. Probability of damage to the National Security cannot be discounted, or

c. Significant activity weakness is revealed, or

24 MAY 1991

- d. Punitive action is appropriate.

Then a JAG Manual investigation will be initiated. JAG investigations will be forwarded via OP-09B to OP-09N.

e. The Preliminary Inquiry will be sent directly to the originator of the material involved, if in Department of Defense, advising that further investigation is being conducted with information copies to OP-09B, OP-09N and NISRA.

f. If the originator of the material is outside of the Department of Defense, send the report to OP-09N who will notify the originator.

6. Preliminary inquiries must be forwarded to the Office of the Assistant Vice Chief of Naval Operations (OP-09B) not later than 3 days after the violation report is signed by OP-09B unless otherwise noted above in paragraph 5. If more time is required to complete the report, notify the OPNAV Security Manager (OP-09B31) in writing of the reason for delay and the expected date of completion.

1603. ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES, AND PUNITIVE ACTIONS

1. Civilian employees are subject to administrative sanctions, civil remedies, and criminal penalties if they knowingly, willfully or negligently disclose classified information to an unauthorized person or knowingly, willfully, or negligently violate provisions of this instruction and the provisions of reference (a) for classification and protection of classified information. Sanctions include, but are not limited to: a warning notice, reprimand, suspension without pay, a forfeiture of pay, removal and discharge. See Civilian Personnel Instruction (CPI) 752 of October 1980 (NOTAL) for a description of adverse personnel actions and their application.

2. Military personnel are subject to punitive action, either in civil courts or under the Uniform Code of Military Justice (UCMJ), as well as administrative sanctions, if they disclose classified information to an unauthorized person or violate provisions of this instruction and the provisions of reference (a) for classification and protection of classified information. When court-martial is recommended as a punitive action for compromise or other security violation, as with court-martial for other reasons, notify the local Judge Advocate General (JAG)

24 MAY 1991

office immediately so they can draw up the charge and specification.

3. Disciplinary action is used primarily to make it clear to the offender, and other personnel, that lax security procedures will not be tolerated. Action taken for involvement in security violations should suit the offense and be applied regardless of rank, rate or grade. Within the Office of the Chief of Naval Operations, the Immediate Offices of the Secretary of the Navy and the Department of the Navy Staff Offices, the minimum corrective action for security violations is the presentation of a non-punitive letter of caution to the individual, military or civilian, responsible.

1604. REVIEW OF VIOLATION REPORTS

The Assistant Vice Chief of Naval Operations (OP-09B) shall review all completed investigation reports to ensure that the findings of the preliminary investigation are complete and appropriate corrective action has been taken to preclude reoccurrence. Where insufficient or inappropriate action appears to have been taken, OP-09B shall recommend further investigation.

24 MAY 1991

CHAPTER 17

TERRORISM

1701. INTRODUCTION

Terrorism is the unlawful use of or threatened use of force or violence by a revolutionary organization against individuals or property, with the intention of coercing or intimidating governments or societies often for political or ideological purposes. Acts of terrorism directed at naval personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage through adverse publicity.

1702. RESPONSIBILITIES

1. The Defense Protective Service (DPS) is responsible for protection of the Pentagon, its occupants and government and private property. The OPNAV Security Manager (OP-09B31), interfaces with DPS and in consonance with guidelines, administers security enforcement procedures within OPNAV and the Secretariat through the Security Coordinators.

2. The OPNAV Security Force under the direction of the OPNAV Security Manager provides physical security for Department of the Navy spaces located within the Pentagon.

3. Each ACNO, DCNO, DSO, ASN and Director of DON Staff Office exercises command responsibilities and security enforcement authority within the spaces of their respective organization.

1703. THREAT CONDITIONS

1. The Joint Chiefs of Staff have established a series of threat conditions and corresponding measures to facilitate inter-service coordination and support U.S. military antiterrorism activities. In the Washington, DC area, these conditions would normally be set and measures implemented by the Commandant of the Naval District of Washington (NDW), based on all threat intelligence available. The remainder of this chapter lists the JCS threat conditions and measures and immediately below the corresponding actions for OPNAV activities in the Pentagon. OPNAV activities located outside the Pentagon will fall under the

24 MAR 88

security plan established by their Building Manager and executed through the DPS.

2. Threat Condition ALPHA. A general warning of possible terrorist activity, the nature and extent of which are unpredictable, where the circumstances do not justify full implementation of the measures contained in THREATCON BRAVO. However, it may be necessary to implement selected measures from THREATCON BRAVO. The measures in this threat condition must be capable of being maintained indefinitely.

ORDERED MEASURE - 1

At regular intervals, remind all personnel, including dependents, to be suspicious and inquisitive about strangers particularly those carrying suitcases or other containers; be alert for unidentified vehicles on, or in the vicinity of Naval installations; and be alert for abandoned parcels or suitcases or any unusual activity.

OPNAV RESPONSE

OPNAV Security Manager (OP-09B31) call each ACNO, DCNO, DSO, ASN, and DON Staff Office Security Coordinator and Provost Marshal (Hendersen Hall). Inform them of the threat condition and measures in effect and provide relevant threat intelligence. Security Coordinators brief their principals and assigned personnel.

ORDERED MEASURE - 2

Keep the Security Officer or other appointed personnel who have access to plans for evacuating buildings and areas in use and for sealing off any areas where an explosion or attack has occurred available at all times. Keep key personnel who may be needed to implement security plans on call.

OPNAV RESPONSE

OPNAV Security Manager and all Security Coordinators are on call. OPNAV Security Manager review Pentagon evacuation plan and OPNAV Security recall bill.

ORDERED MEASURE - 3

Secure buildings, rooms and storage areas not in regular use.

24 MAY 1981

OPNAV RESPONSE

OPNAV Security Manager check in with Security Coordinators to identify vacant DON spaces. OPNAV Security Force Patrols ensure all DON spaces are locked when not in use.

ORDERED MEASURE - 4

Increase security spot checks of vehicles and persons entering the installations and nonclassified areas under the jurisdiction of the installation or command.

OPNAV RESPONSE

Access to the Pentagon is controlled by DPS. DPS alert condition yellow satisfies this measure.

ORDERED MEASURE - 5

Limit access points for vehicles and personnel to commensurate with a reasonable flow of traffic.

OPNAV RESPONSE

Access to the Pentagon and movement within the Pentagon are controlled by DPS. Access to DON spaces is controlled by the Security Coordinator for each space.

ORDERED MEASURE - 6

As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly.

OPNAV RESPONSE

Based on threat intelligence, the OPNAV Security Manager will select one of following measures: 14, 15, 17 or 18. After AVCNO approval, the selected measure will be implemented in DON Pentagon spaces.

ORDERED MEASURE - 7

Review all plans, directives, personnel details and logistic requirements related to the introduction of higher THREATCON.

24 MAY 1991

OPNAV RESPONSE

OPNAV Security Manager and Security Coordinators review plans for implementing higher threat conditions.

ORDERED MEASURE - 8

Review and implement security measures for high-risk personnel.

OPNAV RESPONSE

OPNAV Security Force reviews duress alarm procedures. Based on threat intelligence, identify personnel who may require additional protection. AVCNO approve and arrange protection from Naval Investigative Service Command (NISC).

ORDERED MEASURE - 9

Spare.

OPNAV RESPONSE

Spare.

3. Threat Condition BRAVO. This condition is declared when there is increased and more predictable threat of terrorist activity even though no particular target is identified. The measures in this threat condition must be capable of being maintained for weeks without causing undue hardship, without affecting operation capability and without aggravating relations with local authorities.

ORDERED MEASURE 10

Repeat MEASURE 1 and warn personnel of any other form of attack to be used by terrorists.

OPNAV RESPONSE

Repeat MEASURE 1. OPNAV Security provides any additional threat intelligence and explain additional measures being implemented to all Security Coordinators.

ORDERED MEASURE 11

Keep all personnel involved in implementing anti-terrorist contingency plans on call.

24 MAY 1991

OPNAV RESPONSE

Off duty OPNAV Security and all Security Coordinators are on call.

ORDERED MEASURE 12

Check plans for implementation of the measures contained in the next THREATCON.

OPNAV RESPONSE

OPNAV Security Manager and all Security Coordinators review plans for implementing higher threat conditions.

ORDERED MEASURE 13

Where possible, cars and objects such as crates, trash containers, etc., are to be moved at least 80 feet (25 meters) from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

OPNAV RESPONSE

Keeping the outside of the Pentagon clear is a DPS responsibility, but all hands should be prepared to assist as required. OPNAV Security Manager will coordinate with DPS and keep all hands informed via Security Coordinators. OP-09B32 should ensure that the East Loading Dock is kept clear when not in use.

ORDERED MEASURE 14

Secure and regularly inspect all buildings, rooms and storage areas not in regular use.

OPNAV RESPONSE

Same as MEASURE 3: OPNAV Security Force increase each watch shift to four men and increase frequency of patrols.

ORDERED MEASURE 15

At the beginning and end of each workday and at regular and frequent intervals, inspect for suspicious activity or packages the interior and exterior of buildings in regular use.

24 MAY 1991

OPNAV RESPONSE

All Security Coordinators inspect their spaces at the beginning and end of each workday and alert their people to watch for suspicious packages. OPNAV Security Force shall increase patrols as in MEASURE 14 above. All suspicious packages should be reported to DPS.

ORDERED MEASURE 16

Examine all mail for letter or parcel bombs. This examination is increased above normal.

OPNAV RESPONSE

All incoming mail is currently being x-rayed by the Defense Post Office. OP-09B34 review letter bomb recognition training with all mailroom personnel.

ORDERED MEASURE 17

Check all deliveries to messes, clubs, etc. (Advise dependents to check all home deliveries.)

OPNAV RESPONSE

SECNAV/CNO Flag Mess Officer ensure linen deliveries are checked at the loading dock vice at the mess itself.

ORDERED MEASURE 18

As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs and other soft targets to improve deterrence and defense and build confidence among staff and dependents.

OPNAV RESPONSE

Security of government quarters located on base is the responsibility of the base commander.

ORDERED MEASURE 19

Make staff and dependents aware of the general situation to stop rumors and prevent unnecessary alarm.

24 May 1981

OPNAV RESPONSE

OPNAV Security Manager disseminate relevant threat intelligence via Security Coordinators. If appropriate, issue a bulletin explaining the current situation and protective measures for individuals.

ORDERED MEASURE 20

At an early stage, inform members of local security committees of any action being taken and why.

OPNAV RESPONSE

OPNAV Security Manager contact NDW Operations and Assistant for Administration, Office of the Under Secretary of the Navy for Administration to coordinate activities.

ORDERED MEASURE 21

Upon entry of visitors to the command, physically inspect them and a percentage of their suitcases, parcels and other containers.

OPNAV RESPONSE

Inspection of visitors to Pentagon is a DPS responsibility. DPS alert condition yellow satisfies this measure. OPNAV Security Manager will coordinate with DPS and keep all hands informed.

ORDERED MEASURE 22

Wherever possible, operate random patrols to check vehicles, people and buildings.

OPNAV RESPONSE

As in MEASURES 14 and 15, increase OPNAV Security Force watch shifts to four men each. This will allow a two man team to be out on patrol of OPNAV spaces almost continuously. OPNAV Security Manager may adjust patrol routes and areas based on specific threat intelligence.

ORDERED MEASURE 23

Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked

24 MAY 1991

vehicles and to institute a positive system of checking before they enter and drive cars.

OPNAV RESPONSE

OPNAV Security distribute a bulletin listing security measures individuals should take when they go outside the Pentagon. Remind all hands to lock their cars when parked and to inspect them prior to entry.

ORDERED MEASURE 24

Implement additional security measures for high-risk personnel.

OPNAV RESPONSE

OPNAV Security Manager reviews duress alarm response procedures with personnel having access to these alarms and with any NISC agents assigned. OPNAV Security Manager will review the security measures for high-risk personnel as in MEASURE 8. Recommend changes deemed necessary to AVCNO.

ORDERED MEASURE 25

Brief personnel who may augment the guard force on the use of deadly force.

OPNAV RESPONSE

OPNAV Security Manager will identify personnel who may be needed to augment the guard force, brief them on the threat, and train them in proper response procedures.

ORDERED MEASURE 26

Provide increased security surveillance of waterfront areas including wharfs, piers, caissons, critical communication facilities, assets, etc.

OPNAV RESPONSE

OPNAV Security Manager will notify OPNAV Communication Center of threat condition.

ORDERED MEASURES 27 THROUGH 29

Spare.

24 MAY 1991

OPNAV RESPONSE

Spare.

4. Threat Condition CHARLIE. This condition is declared when an incident occurs or when intelligence is received indicating that some form of terrorist action against the installation or personnel is imminent. Implementation of this measure for more than short periods will probably create hardship and will affect the peacetime activities of the installation and its personnel.

ORDERED MEASURE 30

Continue all THREATCON BRAVO measures or introduce those outstanding.

OPNAV RESPONSE

OPNAV Security Manager review previously implemented procedures; ensure all measures from condition BRAVO are implemented. Promulgate new threat condition and new measures as well as any new threat intelligence to all Security Coordinators. Security Coordinators brief their principals and required personnel.

ORDERED MEASURE 31

Keep all personnel who are responsible for implementing anti-terrorist plans available at their places of duty.

OPNAV RESPONSE

Recall all OPNAV Security Force personnel and all Security Coordinators. Based on threat intelligence, OPNAV Security Manager will determine if guard force augmentation is required.

ORDERED MEASURE 32

Limit access points to absolute minimum.

OPNAV RESPONSE

Control of Pentagon access points is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

24 MAY 1991

ORDERED MEASURE 33

Strictly enforce control of base entry and search a percentage of vehicles.

OPNAV RESPONSE

Control of entry to the Pentagon and vehicle search are DPS responsibilities. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 34

Enforce centralized parking of vehicles away from sensitive buildings.

OPNAV RESPONSE

Control of parking at the Pentagon is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 35

Issue weapons to guards.

OPNAV RESPONSE

Weapons should be issued only to personnel who have been trained in their use. Issue of weapons to anyone outside the OPNAV Security Force must be specifically approved by the AVCNO.

ORDERED MEASURE 36

Introduce increased patrolling of the installation.

OPNAV RESPONSE

OPNAV Security Manager will establish at least one additional patrol team beyond that already established by MEASURE 22. The number and patrol areas of additional teams will be determined based on threat intelligence.

ORDERED MEASURE 37

Protect all designated vulnerable points (VP's) and give special attention to VP's outside naval installations and activities.

24 MAY 1991

OPNAV RESPONSE

Based on threat intelligence, the OPNAV Security Manager will identify any VP's in DON Pentagon spaces and coordinate with DPS for proper protection. He/she will brief AVCNO on VP's and protection plans.

ORDERED MEASURE 38

Erect barriers and obstacles to control traffic flow.

OPNAV RESPONSE

Traffic barriers around the Pentagon are DPS responsibility.

ORDERED MEASURE 39

Spare.

OPNAV RESPONSE

Spare.

5. Threat Condition DELTA. A terrorist attack has occurred or intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

ORDERED MEASURE 40

Continue or introduce all measures listed for THREATCON BRAVO and CHARLIE.

OPNAV RESPONSE

OPNAV Security Manager will review previously implemented procedures; ensure all measures from BRAVO and CHARLIE are implemented. Promulgate new threat condition and new measures as well as any new threat intelligence to all Security Coordinators. Security Coordinators brief their principals and required personnel.

ORDERED MEASURE 41

Augment guard/police forces as necessary.

OPNAV 1000

OPNAV RESPONSE

The OPNAV Security Manager will liaison with DPS to determine their augmentation plan for the Pentagon. Based on threat intelligence, OPNAV Security Manager will develop and propose a plan to AVCNO for stationing any guards required inside DON Pentagon spaces.

ORDERED MEASURE 42

Identify all vehicles already on the installation within operational or mission support areas.

OPNAV RESPONSE

Identification of vehicles is a DPS responsibility but all hands must be prepared to cooperate.

ORDERED MEASURE 43

Search all vehicles and contents entering the complex or installation.

OPNAV RESPONSE

Vehicle search is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 44

Control all base access points and implement positive identification of all personnel.

OPNAV RESPONSE

Control of access to the Pentagon is a DPS responsibility. Positive identification will be achieved by all hands wearing their building pass where it can be easily seen. OPNAV Security Force patrols will verify identity of anyone in a DON space not wearing a valid pass.

ORDERED MEASURE 45

Search all suitcases, briefcases, packages, etc., brought into the installation or command.

24 MAY 1991

OPNAV RESPONSE

Search of packages entering the Pentagon is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 46

Control access to all areas under the jurisdiction of the naval installation or command concerned.

OPNAV RESPONSE

Control of access to the Pentagon is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 47

Make frequent checks of the exterior of buildings and parking areas.

OPNAV RESPONSE

The exterior of the Pentagon and parked cars is a DPS responsibility. OPNAV Security Manager will liaison with DPS and keep AVCNO and all Security Coordinators advised.

ORDERED MEASURE 48

Minimize all administrative journeys and visits.

OPNAV RESPONSE

ACNOs, DCNOs, DSOs, SECNAV, ASNs and Directors of DON Staff Offices minimize travel for all hands.

ORDERED MEASURE 49

Consult local authorities about closing public (and military) roads and facilities that might make sites vulnerable to terrorist attack.

24 MAY 1991

OPNAV RESPONSE

DPS would liaison with local police to effect the closing of roads. OPNAV Security Manager will liaison with DPS and keep all hands informed of any road closings.

ORDERED MEASURE 50

Man posts as necessary to prevent attack against vulnerable facilities outside the base boundaries.

OPNAV RESPONSE

OPNAV Security Manager coordinate with DPS.

1704. BOMB THREAT

DPS has the responsibility for investigating bomb threats within the Pentagon. They will not be able to perform this task successfully unless the person receiving the call takes proper action and gets as much information as possible. To ensure that OPNAV personnel answering telephones take proper action while under the stress of a bomb threat, a Bomb Threat Card (FBI Form 2-182a) should be used. OPNAV Security distributes these forms. Bomb threats in the Pentagon should be reported to DPS at x75555.

24 MAY 1991

CHAPTER 18

LOSS PREVENTION

1801. BASIC POLICY

1. Loss prevention is concerned with preventing loss of supplies, tools, equipment or other materials in use, storage, transit and during the issue process. Concern is not only focused on the threat of criminal activity and acts of wrongdoing by forces external to the organizational unit, it also specifically addresses internal causes: theft and pilferage by those who have authorized access, inattention to physical security practices and procedures, and disregard for property controls and accountability.

2. Each employee, both civilian and military must be indoctrinated in procedures preventing property losses including his/her personal responsibility for the care and protection of government property. All government property must be accounted for and cannot simply be moved from office to office. This causes an undue amount of reported losses and can be corrected easily by requesting supply transfer custody to the new office. Steps taken to prevent loss include:

a. Do not leave government equipment or supplies in passageways.

b. Ensure equipment being removed from the premises are properly documented with property passes.

c. Ensure spaces are locked when unoccupied.

d. Turn in all equipment that is in excess.

e. Do not keep an excessive number of supplies onboard.

3. OPNAVINST 5530.14B and SECNAVINST 5500.4F (NOTAL) establish the requirements for OPNAV Security to report incidents of missing, lost, stolen or recovered government property, which meets the following criteria:

a. Sensitive items; e.g., drugs, precious metals, alcohol, when any discrepancy exists, regardless of dollar value.

b. Classified items regardless of dollar value.

24 MAY 1991

c. Arms, ammunition, and explosives regardless of dollar value.

d. Pilferable, valuable and attractive items which are easily convertible to personal use, e.g., hand tools, individual clothing, office machines, photographic equipment, etc., when the value of line item discrepancy is \$800 or more.

e. Any discrepancy or repetitive losses when there is an indication or suspicion of fraud, theft, or negligence.

f. Any bar-coded item.

Any person assigned to OPNAV, SECNAV or DON Staff Offices must immediately notify their directorate's Supply or Equipment Coordinator of any loss. The coordinator will report the loss to the respective supply office (Supply and Space Control Branch OP-09B32 for OPNAV and Secretariat Services Division for SECNAV Staff Offices). Supply will provide a DD Form 200 Report of Survey which is to be completed as indicated in paragraph 1802.

1802. DD 200 PREPARATION

The DD 200 is used to document the Report of Survey and certify the survey process when government property is gained or lost. This form is the official document to support establishment of debts, relief from accountability, and adjustment to accountable records for Supply System Stock and Property Book Material. Blocks 1 through 8 should be completed by the appointed Supply Coordinator of the affected directorate. Specific preparation instructions for the remaining blocks of the DD 200 are provided below:

<u>Block</u>	<u>Entry Instruction</u>
--------------	--------------------------

9	Circumstances - Check the appropriate block. Provide complete statement of facts which should include but not be limited to the date, place of the incident, name grade, SSN of all persons involved. The statement must answer the five basic questions of who, what, when, where and how. The signature and typed name and rank/rate of the individual performing the research (identifying the <u>unresolved</u> discrepancy) will be included in the lower right-hand space of this block.
---	--

~~SECRET~~

<u>Block</u>	<u>Entry Instructions</u>
10	Corrective/Preventive Actions - when applicable, provide corrective actions and describe measures to prevent future occurrences.
11	Supervisor of the individual(s) performing the research documented in blocks 9 and 10 signs this block.
12	Responsible Officer - The form is returned to the Supply Coordinator of the affected directorate. The Supply Coordinator reviews the information, signs and forwards it to the Appointing Official (Executive Assistant for the affected OPNAV code or the Administrative Officer for SECNAV Staff Offices). Blocks 14 through 17 are completed next.
13	Accountable Officer - Signature of the individual appointed to maintain stock, property, and financial records. OP-09B3 for OPNAV or the Administrative Officer for SECNAV Staff Offices. This block is completed after blocks 14 through 17. The form is then forwarded to the Approving Official (OP-09B).
14a	<p>This block will only be completed when personal responsibility is evident.</p> <p>The Survey Officer is appointed by the Appointing Official (see block 17) and must be someone outside the chain of command of persons completing/signing blocks 1 through 12.</p> <p>The Survey Officer must provide findings and recommendations based on the facts established through research/investigation.</p>
14b	<p>This block will <u>only</u> be completed when personal responsibility is evident.</p> <p>Dollar Amount of Loss or Gain - The Survey Officer should take into consideration the standard price of the lost or gained property when completing this block.</p>
14c	Not applicable.

24 MAR 1

<u>Block</u>	<u>Entry Instructions</u>
14d	<p>This block will <u>only</u> be completed when personal responsibility is evident.</p> <p>Government Loss/Gain - The Survey Officer should compute the financial loss or gain to the government.</p>
15	<p>This block will <u>only</u> be completed when personal responsibility is evident.</p> <p>Survey Officer - Signature of the individual appointed to perform the survey and compute the loss or gain to the government.</p>
16	<p>This block will <u>only</u> be completed when personal responsibility is evident.</p> <p>Individual Charged - If the individual charged refuses to sign this block, the refusal should be noted.</p>
17	<p>Appointing Official - Signature of the individual who assigns the survey. The Appointing Official is the Executive Assistant of the affected OP-Code or the Administrative Officer for the affected SECNAV Staff Office.</p>
18	<p>Approving official - Signature of the individual responsible for approving/disapproving the financial liability or relieving responsibility. (OP-09B)</p>

CHAPTER 19

(A)

EMERGENCY PROCEDURES AND NOTIFICATIONS

1901. PURPOSE

To establish policy and standardize requirements for emergency procedures and notification requirements for personnel on the Pentagon Reservation. For those employees housed in other buildings in the National Capital Region these procedures are outlined by the respective building manager.

1902. PROCEDURES

1. DUTY TO REPORT

Occupants of facilities on the Pentagon Reservation shall promptly report all crimes and suspicious circumstances occurring on the Pentagon Reservation to the Defense Protective Service (DPS) telephone number, 703-697-5555 and then to the OPNAV Security Operation Center on 703-695-3667. The DPS Communications Center shall dispatch a police officer to the scene of the offense and/or incident to conduct an investigation.

2. FIRE OR SMOKE

Any person, who observes fire or smoke, should activate the nearest alarm box. If the person smells something burning, he or she shall notify the DPS at 703-695-5555, and provide the room number or location of the possible fire.

3. MEDICAL EMERGENCIES

Notify the DPS on 703-697-5555. The DPS shall contact the appropriate medical service.

4. SUSPICIOUS PERSONS AND/OR PACKAGES

Any person discovering a suspicious package or observing a suspicious person shall notify the DPS, on 703-697-5555. Do not touch or move any suspicious articles.

17 NOV 1997

5. NUISANCE CALLS, PERSONS, OR LETTERS

Unsolicited contacts may be in person, in writing, or by telephone. Information may be received about individuals or organizations that may pose a threat to the safety and security of Government officials. Prompt notification should be given to DPS of all threats. Contacts that do not contain a direct threat to do harm but indicate an intent to embarrass or harass should not be ignored. Chronic letter writers and multiple telephone calls from an individual generally create more of a nuisance than a threat. However, each occurrence should be monitored closely to determine any attitude changes in individuals.

6. BOMB THREATS

Any person receiving a bomb threat should attempt to record the following and immediately telephone the DPS on 703-697-5555:

- a. Exact words of caller.
- b. Time the device is to explode.
- c. Location of the device.
- d. Time and date of call.
- e. Name of caller.
- f. Sex of caller.
- g. Accents or dialects.
- h. Age (i.e. young or old).
- i. Any background noises heard over the telephone.

7. HOSTAGE OR TERRORIST INCIDENT

Notify DPS on 703-697-5555.

8. THREATCON

Refer to Chapter 17 of this instruction.

17 NOV 1937

1903. NOTIFICATIONS

1. The OPNAV Security Operation Center (SOC) receives from DPS, via the DPS Digital Conferencing Switching System (DCSS), emergency alert information on incidents occurring on the Pentagon Reservation. The OPNAV Security Manager, based on the actual threat received, will through the SOC immediately notify all command personnel by the following means:

a. Telephonic notification to all Principle Officials, Security Coordinators and Navy Command Center.

b. Red Flash message from SOC via Department of Navy Information Project Office (DONINPO) to all computer account holders.

c. If all telephone and computer lines are down, the OPNAV Security Manager will dispatch Navy Security Force personnel throughout the Pentagon hallways with multi-sound megaphones to pass the information.

2. OPNAV SOC will pass on available details from DPS or other sources without jeopardizing either time or situation integrity. Due to the large number of personnel to notify, the SOC will not have time to answer questions at time of call. Incoming calls must be held to a minimum and pass only critical information during these situations.

3. When a specific office receives notification, that office must alert personnel in adjacent spaces which in turn passes the word throughout SECNAV/USMC/OPNAV spaces.

24 MAR 1991

APPENDIX A

PROCUREMENT OF FORMS

1. The forms listed below are prescribed by this instruction and may be procured as indicated:

a. The following forms may be ordered from local supply offices or the General Services Administration:

Standard Form 700	Security Container Information	7540-01-214-5372
Standard Form 701	Activity Security Checklist	7540-01-213-7899
Standard Form 702	Security Container Check Sheet	7540-01-213-7900
Standard Form 703	Top Secret Cover Sheet	7540-01-213-7901
Standard Form 704	Secret Cover Sheet	7540-01-213-7902
Standard Form 705	Confidential Cover Sheet	7540-01-213-7903
Standard Form 706	Top Secret ADP Media Label	7540-01-207-5536
Standard Form 707	Secret ADP Media Label	7540-01-207-5537
Standard Form 708	Confidential ADP Media Label	7540-01-207-5538
Standard Form 709	Classified ADP Media Label	7540-01-207-5540
Standard Form 710	Unclassified ADP Media Label	7540-01-207-5539
Standard Form 711	Classification Authority/ Declassification Instructions ADP Media Label	7540-01-207-5541

b. The following forms may be ordered from local supply offices or the Navy supply systems per NAVSUP P-2002:

DD Form 200	Report of Survey	0102-LF-000-2001
DD Form 254	Contract Security Classification	0102-LF-000-2540
OPNAV 5216/10	Correspondence/Material Control (4 Pt)	0107-LF-052-1650
OPNAV 5511/10	Record of Receipt	0107-LF-002-2300
OPNAV 5511/11	Notice of Change in Classification	0107-LF-786-1000
OPNAV 5511/12	Classified Material Destruction Report	0107-LF-055-1160
OPNAV 5511/13	Record of Disclosure	0107-LF-055-1165
OPNAV 5511/14	Security Termination Statement	0107-LF-055-1171
OPNAV 5511/51	Security Discrepancy Notice	0107-LF-055-5355
OPNAV 5521/27	Visit Request	0107-LF-055-2235

c. DOE F5631.20 may be ordered from the Chief of Naval Operations (CNO) (OP-09B31D), Room 4A662, Pentagon, Department of the Navy, Washington, DC 20350-2000.

d. The forms listed below may be ordered from the Chief of Naval Operations (OP-09B31F), Room 4A654, Pentagon, Department of the Navy, Washington, DC 20350-2000:

OPNAVINST 5510.60L

241

FBI Form 2-182a
HQ-NDW 5560/1
OPNAV 5512-6

Bomb Threat Card
Automobile Registration Request
Alarmed Area Access List

e. The forms listed below are controlled and issued from the offices and Pentagon room numbers indicated. Blank forms are not disseminated.

DD Form 2249	DOD Building Pass Request	OP-09B31D (4A662)
DD Form 2501	Courier Authorization Card	OP-09B31 (4A662)
GSA Optional Form 7	Property Pass	OP-09B32 (5E577) OP-09B31D (4A654)
OPNAV 5510/413	Personnel Security Action Request	OP-09B31D (4A662)
OPNAV 5511/5	Security Violation Report	OP-09B31 (4A662)
Standard Form 312	Classified Information Nondisclosure Agreement	OP-09B31D (4A662)

f. The forms listed below are available in local supply rooms (for CNO personnel, OP-09B32, Room 5E568, Pentagon - for SECNAV personnel, Secretariat Services Support Division, Room 5E773, Pentagon):

OPNAV 5511/57	Classified Material Destruction Manifest
OPNAV 5900/3	Office Services Request